

Jonathan M. Rotter (SBN 234137)  
Pavithra Rajesh (SBN 323055)  
**GLANCY PRONGAY & MURRAY LLP**  
1925 Century Park East, Suite 2100  
Los Angeles, California 90067  
Telephone: (310) 201-9150  
Facsimile: (310) 201-9160  
jrotter@glancylaw.com  
prajesh@glancylaw.com

Daniel O. Herrera (*pro hac vice* anticipated)  
Nickolas J. Hagman (*pro hac vice* anticipated)  
**CAFFERTY CLOBES MERIWETHER  
& SPRENGEL LLP**  
135 S. LaSalle, Suite 3210  
Chicago, Illinois 60603  
Telephone: (312) 782-4880  
Facsimile: (312) 782-4485  
dherrera@caffertyclobes.com  
nhagman@caffertyclobes.com

*Attorneys for Plaintiffs and the Proposed Class*

[Additional Counsel on Signature Page]

**UNITED STATES DISTRICT COURT  
FOR THE CENTRAL DISTRICT OF CALIFORNIA**

SHANNON MASSER DOWNS, M.B.,  
a minor, by and through her legal  
guardian, Shannon Masser Downs, and  
MARIA HINESTROSA, individually,  
and on behalf of all others similarly  
situated,

Plaintiffs,

v.

REGAL MEDICAL GROUP, INC.,  
LAKESIDE MEDICAL  
ORGANIZATION, A MEDICAL  
GROUP, INC., AFFILIATED  
DOCTORS OF ORANGE COUNTY  
MEDICAL GROUP, INC., and  
GREATER COVINA MEDICAL  
GROUP, INC.

Defendants.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

1 Plaintiffs Shannon Masser Downs, and M.B., a minor, by and through her legal  
 2 guardian Shannon Masser Downs, and Maria Hinestrosa (collectively, “Plaintiffs”),  
 3 individually, and on behalf of all others similarly situated, bring this action against  
 4 Regal Medical Group, Inc., Lakeside Medical Organization, A Medical Group, Inc.,  
 5 Affiliated Doctors of Orange County Medical Group, Inc., and Greater Covina  
 6 Medical Group, Inc., (collectively, “Regal” or “Defendants”), by and through their  
 7 attorneys, and allege, based upon personal knowledge as to their own actions, and  
 8 based upon information and belief as to all other matters, as follows:

### 9 **INTRODUCTION**

10 1. Defendants are full-service medical groups providing healthcare services  
 11 through its network of medical groups in Southern California.<sup>1</sup>

12 2. As one of the largest physician-led healthcare networks in Southern  
 13 California, Defendants contract with doctors, hospitals, and urgent care centers to  
 14 provide patients with options for managing their health.<sup>2</sup>

15 3. In doing so, Defendants collect, maintain, and store their patients’ highly  
 16 sensitive personal and medical information including, but not limited to: Social  
 17 Security numbers, dates of birth, full names, addresses, telephone numbers,  
 18 information regarding medical treatment and diagnosis, prescription data, laboratory  
 19 test results, radiology reports, health plan member numbers, and other protected  
 20  
 21

---

22 <sup>1</sup> See *About Us*, Regal Medical Group, <https://www.regalmed.com/about-us/> (last  
 23 accessed Feb. 22, 2023); *About Us*, Lakeside Community Healthcare,  
 24 <https://www.lakesidemed.com/about-us/> (last accessed Feb. 22, 2023); *About Us*,  
 25 ADOC Medical Group, <https://www.adoc.us/about-us/> (last accessed Feb. 22, 2023);  
 26 *About Us*, Greater Covina Medical Group Inc., <https://www.gcmg.org/about-us/> (last  
 accessed Feb. 22, 2023).

27 <sup>2</sup> *About Us*, Regal Medical Group, <https://www.regalmed.com/about-us/> (last  
 28 accessed Feb. 22, 2023).

1 health information (“personally identifying information” or “PII”).<sup>3</sup>

2 4. Although Defendants are sophisticated medical entities providing  
3 services to hundreds of thousands of patients, Defendants failed to invest in adequate  
4 data security, thereby allowing hackers to exfiltrate the highly-sensitive personal and  
5 medical information of approximately 3,300,638 individuals, including the Plaintiffs  
6 and Class members.<sup>4</sup> As a direct, proximate, and foreseeable result of Defendants’  
7 failure to implement reasonable security protections sufficient to prevent an eminently  
8 avoidable cyberattack, unauthorized actors compromised Defendants’ network and  
9 accessed millions of patient files containing highly-sensitive PII.<sup>5</sup>

10 5. Specifically, began on or around December 1, 2022, Defendants’  
11 patients’ sensitive personal and medical data was compromised when unauthorized  
12 actors were able to breach Defendants’ network and access files containing  
13 approximately 3,300,638 individual’s PII (the “Data Breach”).<sup>6</sup>

14  
15 <sup>3</sup> *Submitted Breach Notification Sample*, Office of the Attorney General California  
16 Department of Justice, <https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf> (last accessed Feb. 22, 2023).

18 <sup>4</sup> *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected*  
19 *Health Information*, U.S. Department of Health and Human Services Office for Civil  
20 Rights, [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (las accessed Feb. 22,  
21 2023); *see 3.3 Million Impacted by Ransomware Attack at California Healthcare*  
22 *Provider*, Security Week, [https://www.securityweek.com/3-3-million-impacted-by-](https://www.securityweek.com/3-3-million-impacted-by-ransomware-attack-at-california-healthcare-provider/)  
23 [ransomware-attack-at-california-healthcare-provider/](https://www.securityweek.com/3-3-million-impacted-by-ransomware-attack-at-california-healthcare-provider/) (last accessed Feb. 22, 2023).

24 <sup>5</sup> *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected*  
25 *Health Information*, U.S. Department of Health and Human Services Office for Civil  
26 Rights, [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (las accessed Feb. 22,  
27 2023); *see 3.3 Million Impacted by Ransomware Attack at California Healthcare*  
28 *Provider*, Security Week, [https://www.securityweek.com/3-3-million-impacted-by-](https://www.securityweek.com/3-3-million-impacted-by-ransomware-attack-at-california-healthcare-provider/)  
[ransomware-attack-at-california-healthcare-provider/](https://www.securityweek.com/3-3-million-impacted-by-ransomware-attack-at-california-healthcare-provider/) (last accessed Feb. 22, 2023).

<sup>6</sup> *Submitted Breach Notification Sample*, Office of the Attorney General California  
Department of Justice,

6. Despite the fact that many of the categories of PII exposed in the Data Breach, such as Social Security numbers and medical information, cannot be changed, Defendants failed to detect the breach until a week later, on or around December 8, 2022, and failed to notify affected individuals until on or around February 1, 2023—approximately two months after unauthorized individuals accessed Plaintiffs’ and current and former patients’ highly sensitive PII stored on Defendants’ systems.<sup>7</sup>

7. Defendants’ failure to promptly notify Plaintiffs and Class members that their PII was exfiltrated due to Defendants’ security failures virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse and/or disseminate that PII before Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

8. Defendants failed to take sufficient and reasonable measures to safeguard their data security systems and protect highly sensitive data in order to prevent the Data Breach from occurring; to disclose to current and former patients the material fact that it lacked appropriate data systems and security practices to secure PII and medical information; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Due to Defendants’ failures, Plaintiffs and approximately 3,300,638 individuals suffered substantial harm and injury.

---

<https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf> (last accessed Feb. 22, 2023); see *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Department of Health and Human Services Office for Civil Rights, [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (last accessed Feb. 22, 2023).

<sup>7</sup> *Submitted Breach Notification Sample*, Office of the Attorney General California Department of Justice, <https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf> (last accessed Feb. 22, 2023).

1           9. As a result of Defendants' negligent, reckless, intentional, and/or  
2 unconscionable failure to adequately satisfy its contractual, statutory, and common-  
3 law obligations, Plaintiffs' and Class members' PII was accessed and acquired by  
4 unauthorized third-parties for the express purpose of misusing the data and causing  
5 further irreparable harm to the personal, financial, reputational, and future well-being  
6 of Defendants' current and former patients. Plaintiffs and Class members face the  
7 real, immediate, and likely danger of identity theft and misuse of their PII, especially  
8 because their PII was specifically targeted by malevolent actors.

9           10. Plaintiffs and Class members suffered injuries as a result of Defendants'  
10 conduct including, but not limited to: lost or diminished value of their PII; out-of-  
11 pocket expenses associated with the prevention, detection, and recovery from identity  
12 theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated  
13 with attempting to mitigate the actual consequences of the Data Breach, including but  
14 not limited to the loss of time needed to take appropriate measures to avoid  
15 unauthorized and fraudulent charges; time needed to change usernames and  
16 passwords on their accounts; time needed to investigate, correct and resolve  
17 unauthorized access to their accounts; time needed to deal with spam messages and  
18 e-mails received subsequent to the Data Breach; charges and fees associated with  
19 fraudulent charges on their accounts; and the continued and increased risk of  
20 compromise to their PII, which remains in Defendants' possession and is subject to  
21 further unauthorized disclosures so long as Defendants fail to undertake appropriate  
22 and adequate measures to protect their PII. These risks will remain for the lifetimes  
23 of Plaintiffs and the Class.

24           11. Accordingly, Plaintiffs bring this action on behalf of all those similarly  
25 situated to seek relief from Defendants' failure to reasonably safeguard Plaintiffs' and  
26 Class members' PII; their failure to reasonably provide timely notification that  
27 Plaintiffs' and Class members' PII had been compromised by an unauthorized third  
28 party; and for intentionally and unconscionably deceiving Plaintiffs and Class

1 members concerning the status, safety, location, access, and protection of their PII.

2 **PARTIES**

3 ***Plaintiffs Shannon Masser Downs and M.B.***

4 12. Plaintiff Shannon Masser Downs is a resident and citizen of California,  
5 residing in Valencia, California. Plaintiff Shannon Downs received from Defendants  
6 a letter concerning the data breach dated February 1, 2023.

7 13. Plaintiff M.B., a minor, is a resident and citizen of California, residing  
8 in Valencia, California. Plaintiff M.B. received from Defendants a letter  
9 concerning the data breach dated February 1, 2023.

10 ***Plaintiff Maria Hinestrosa***

11 14. Plaintiff Hinestrosa is a resident and citizen of California, residing in Los  
12 Angeles, California. Plaintiff Hinestrosa received a data breach letter from  
13 Defendants that was dated February 1, 2023.

14 ***Defendant Regal Medical Group, Inc.***

15 15. Defendant Regal Medical Group, Inc. is a healthcare network connecting  
16 patients to doctors, hospitals, and urgent care centers organized under the laws of the  
17 State of California with its principal place of business at 3115 Ocean Front Walk, 301,  
18 Marina Del Rey, CA, 90292.

19 ***Defendant Lakeside Medical Organization, A Medical Group, Inc.***

20 16. Defendant Lakeside Medical Organization, A Medical Group, Inc. is a  
21 healthcare network connecting patients to doctors, hospitals, and urgent care centers  
22 organized under the laws of the State of California with its principal place of business  
23 at 3115 Ocean Front Walk, 301, Marina Del Rey, CA, 90292.

24 ***Defendant Affiliated Doctors of Orange County Medical Group, Inc.***

25 17. Defendant Affiliated Doctors of Orange County Medical Group, Inc. is  
26 a healthcare network connecting patients to doctors, hospitals, and urgent care centers  
27 organized under the laws of the State of California with its principal place of business  
28 at 3115 Ocean Front Walk, 301, Marina Del Rey, CA, 90292.

1           ***Defendant Greater Covina Medical Group, Inc.***

2           18. Defendant Greater Covina Medical Group, Inc. is a practice association  
3 with a healthcare network connecting patients to doctors and specialists organized  
4 under the laws of the State of California with its principal place of business at 605  
5 East Badillo Street, 300, Covina, CA, 91723.

6                           **JURISDICTION AND VENUE**

7           19. This Court has subject-matter jurisdiction pursuant to the Class Action  
8 Fairness Act of 2005 (“CAFA”), 28 U.S.C. § 1332(d)(2), because this is a class action  
9 in which the matter in controversy exceeds the sum of \$5,000,000, the number of class  
10 members exceeds 100, and at least one member of the Class is a citizen of a state  
11 different from Defendants. This Court also has supplemental jurisdiction pursuant to  
12 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or  
13 controversy.

14           20. This Court has personal jurisdiction over Defendants because  
15 Defendants are authorized to and regularly conduct business in California, and is  
16 headquartered in this District.

17           21. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a  
18 substantial part of the events or omissions giving rise to Plaintiffs’ and Class  
19 members’ claims occurred in this District.

20                           **FACTUAL ALLEGATIONS**

21           **A. Defendants – Background**

22           22. Defendants are affiliated full-service medical groups that provide a  
23 variety of health care services including medical services and treatment from primary  
24 care physicians, specialists, hospitals, urgent care centers and labs and care resources  
25 including exercise programs, cooking classes, condition management programs and  
26  
27  
28



1 individual coaching.<sup>8</sup> Defendants represent to their patients that they will “help  
2 organize and coordinate all of your care, and provide valuable health programs and  
3 services.”<sup>9</sup>

4 23. As part of their medical and business operations, Defendants collect,  
5 maintain, and store the highly sensitive PII and medical information provided by their  
6 current and former patients, including but not limited to: Social Security numbers,  
7 dates of birth, full names, addresses, telephone numbers, information regarding  
8 medical treatment and diagnosis, prescription data, laboratory test results, radiology  
9 reports, and health plan member numbers.

10 24. On information and belief, at the time of the Data Breach, Defendants  
11 failed to implement necessary data security safeguards, which resulted in  
12 unauthorized third parties accessing the PII of approximately 3,300,608 current and  
13 former patients.<sup>10</sup>

14 25. Current and former patients of Defendants, such as Plaintiffs and Class  
15 members, allowed their PII to be made available to Defendants with the reasonable  
16 expectation that Defendants would comply with its obligation to keep their sensitive  
17 and personal information, including their PII, confidential and secure from illegal and  
18 unauthorized access, and that Defendants would provide them with prompt and  
19 accurate notice of any unauthorized access to their PII.

20 26. Unfortunately for Plaintiffs and Class members, Defendants failed to  
21

---

22 <sup>8</sup> *About Us*, Regal Medical Group, <https://www.regalmed.com/about-us/> (last  
23 accessed Feb. 22, 2023).

24 <sup>9</sup> *About Us*, Regal Medical Group, <https://www.regalmed.com/about-us/> (last  
25 accessed Feb. 22, 2023).

26 <sup>10</sup> *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected*  
27 *Health Information*, U.S. Department of Health and Human Services Office for Civil  
28 Rights, [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf) (last accessed Feb. 22,  
2023).



1 carry out their duty to safeguard sensitive PII and provide adequate data security, thus  
 2 failing to protect Plaintiffs and Class members from the exfiltration of their PII during  
 3 the Data Breach.

#### 4 **B. The Data Breach**

5 27. Defendants disclosed in a Notice sent on or about February 1, 2023, to  
 6 Plaintiffs and other affected individuals that they were affected by a “ransomware  
 7 cyberattack” in which an unauthorized third party accessed Defendants’ servers,  
 8 installed malware on some of Defendants’ servers, and exfiltrated data concerning  
 9 Defendants’ current and former patients. *See* Notice of Data Breach, attached hereto  
 10 as **Exhibit A**. Further, Defendants acknowledge that the unauthorized actor was able  
 11 to exfiltrate Plaintiffs’ and Class members’ PII, Social Security numbers, and medical  
 12 information.

13 28. Defendants further admitted that employees began experiencing  
 14 “difficulty in accessing some of [Defendants’] servers” on December 2, 2022. *See id.*  
 15 Despite experiencing the effects of the Data Breach on or about December 2, 2022,  
 16 Defendants did not discover the Data Breach until December 8, 2022. *Id.*

17 29. Defendants failed to disclose to Plaintiffs and other victims of the Data  
 18 Breach when the unauthorized third party first gained access to Defendants’ systems  
 19 and how long the unauthorized actor had access to Plaintiffs’ and Class members’  
 20 information. Instead, Defendants admitted to the Office of the California Attorney  
 21 General that the unauthorized actor(s) had unfettered access to Defendants’ computer  
 22 systems, and Plaintiffs’ and other patients’ PII, Social Security numbers, and other  
 23 medical information.<sup>11</sup>

24 30. Defendants assert that upon discovering the Data Breach, it “worked

---

25  
 26 <sup>11</sup> *Submitted Breach Notification Sample*, Office of the Attorney General California  
 27 Department of Justice,  
 28 <https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf> (last accessed Feb. 22, 2023).

1 with [its] vendors to efficiently restore access to [its] systems and to analyze the  
 2 impacted data.” *See* Exhibit A. However, Defendants were not able to secure its  
 3 computer systems until on or after December 8, 2022, seven days after the Data  
 4 Breach occurred, and six days after first experiencing issues related to the Data  
 5 Breach.<sup>12</sup> Defendants failed to disclose to Plaintiffs and Class members that  
 6 Defendants were unable to quickly remove the hacker’s access to Defendants’  
 7 computer systems. *See* Exhibit A.

8 31. Despite discovering the Data Breach on December 8, 2022, and  
 9 confirming that the unauthorized actor accessed and exfiltrated patients’ PII, Social  
 10 Security numbers, and medical records, Defendants delayed sending individualized  
 11 notice to affected patients until on or after February 1, 2023. *See* Exhibit A.

12 32. During the time that the unauthorized individuals had unrestricted access  
 13 to Defendants’ network, they were able to access and acquire personal, sensitive, and  
 14 protected PII and medical information belonging to over 3,300,608 current and former  
 15 patients of Defendants.

### 16 **C. Defendants’ Many Failures Both Prior to and Following the Breach**

17 33. Defendants could have prevented this Data Breach by properly  
 18 encrypting or otherwise protecting their equipment and network files containing PII.

19 34. To be sure, collecting, maintaining, and protecting PII is vital to virtually  
 20 every aspect of Defendants’ operations as a medical group.

21 35. Despite such importance, Defendants failed to detect that their own data  
 22 systems were compromised until on or around December 8, 2022.<sup>13</sup>

23 36. Moreover, when Defendants finally acknowledged that they had

---

24 <sup>12</sup> *Id.*

25  
 26 <sup>13</sup> *Submitted Breach Notification Sample*, Office of the Attorney General California  
 27 Department of Justice,  
 28 <https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf> (last accessed Feb. 22, 2023).

1 experienced a breach, they failed to fully inform affected individuals of the length of  
2 time that the unauthorized actors had access to their PII, or even the full extent of the  
3 PII that was accessed during the Data Breach.

4 37. Defendants' failure to properly safeguard Plaintiffs' and Class members'  
5 PII and medical information allowed the unauthorized actors to access this highly  
6 sensitive PII and medical information, and Defendants' failure to timely notify  
7 Plaintiffs and other victims of the Data Breach that their PII had been misappropriated  
8 precluded them from taking meaningful steps to safeguard their identities prior to the  
9 dissemination of their PII.

10 38. The Data Breach also highlights the inadequacies inherent in  
11 Defendants' network monitoring procedures. If Defendants had properly monitored  
12 their cyber security systems, they would have prevented the Data Breach, discovered  
13 the Data Breach sooner, and/or have prevented the hackers from exfiltrating PII and  
14 medical information.

15 39. Defendants' delayed response only further exacerbated the consequences  
16 of the Data Breach brought on by its systemic IT failures.

17 40. First, Defendants failed to timely secure their computer systems to  
18 protect their current and former patients' PII and medical information. Defendants  
19 allowed the unauthorized actors to continue to have unfettered access to Defendants'  
20 systems for seven days—six days after Defendants first began experiencing issues  
21 related to the Data Breach—until Defendants finally discovered the Data Breach.

22 41. Second, Defendants failed to timely notify affected individuals,  
23 including Plaintiffs and Class members, that their highly-sensitive PII had been  
24 accessed by unauthorized third parties. Defendants waited two months after  
25 discovering the Data Breach to provide notice to the victims of the Data Breach that  
26 their PII had been compromised.

27 42. Third, Defendants made no effort to protect Plaintiffs and the Class from  
28 the long-term consequences of Defendants' acts and omissions. Although the Notice

1 offered victims one-year of complimentary Norton LifeLock credit monitoring,  
2 Plaintiffs' and Class members' PII, including their Social Security numbers, cannot  
3 be changed and will remain at risk long beyond one year. As a result, Plaintiffs and  
4 the Class will remain at a heightened and unreasonable risk of identity theft for the  
5 remainder of their lives.

6 43. In short, Defendants' myriad failures, including the failure to timely  
7 detect the Data Breach and to notify Plaintiffs and Class members with reasonable  
8 timeliness that their personal and medical information had been exfiltrated due to  
9 Defendants' security failures, allowed unauthorized individuals to access and  
10 misappropriate Plaintiffs' and Class members' PII for months before Defendants  
11 finally granted victims the opportunity to take proactive steps to defend themselves  
12 and mitigate the near- and long-term consequences of the Data Breach.

#### 13 **D. Data Breaches Pose Significant Threats**

14 44. Data breaches have become a constant threat that, without adequate  
15 safeguards, can expose personal data to malicious actors. It is well known that PII,  
16 including Social Security numbers in particular, is an invaluable commodity and a  
17 frequent target of hackers.

18 45. In 2018, the Identity Theft Resource Center and CyberScout Annual  
19 End-of-Year Data Breach Report revealed a 126% increase in exposed data.<sup>14</sup>  
20 Between January and July 2019, more than 31.6 million healthcare records were  
21 exposed in data security incidents—more than double the total amount of healthcare  
22 data breaches for all of 2018.<sup>15</sup>

23  
24 <sup>14</sup> *2018 End of Year Data Breach Report*, Identity Theft Resource Center, available at  
25 [https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC\\_2018-End-of-](https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf)  
26 [Year-Aftermath\\_FINAL\\_V2\\_combinedWEB.pdf](https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf) (last accessed July 20, 2022).

27 <sup>15</sup> Steve Adler, *First Half of 2019 Sees 31.6 Million Healthcare Records Breached*,  
28 HIPAA Journal (Aug. 2, 2019), available at: [https://www.hipaaajournal.com/first-half-](https://www.hipaaajournal.com/first-half-of-2019-sees-31-million-healthcare-records-breached)  
[of-2019-sees-31-million-healthcare-records-breached](https://www.hipaaajournal.com/first-half-of-2019-sees-31-million-healthcare-records-breached).

1           46. In fact, Statista, a German entity that collects and markets data relating  
 2 to, among other things, data breach incidents and the consequences thereof, estimates  
 3 that the annual number of data breaches occurring in the United States increased by  
 4 approximately 692% between 2005 and 2018, a year during which over 446.5 million  
 5 personal records were exposed due to data breach incidents.<sup>16</sup> Conditions have only  
 6 worsened since: Statista estimates that “[i]n 2019, the number of data breaches in the  
 7 United States amounted to 1,473 with over 164.68 million sensitive records  
 8 exposed[,]” and that “[i]n the first half of 2020, there were 540 reported data  
 9 breaches.”<sup>17</sup>

10           47. Data breaches are a constant threat because of the price that PII are sold  
 11 for on the dark web. According to Experian, medical records sell on the dark web for  
 12 prices that are hundreds or thousands of times the price of basic personal or financial  
 13 information.<sup>18</sup> For the individual, identity theft causes “significant negative financial  
 14 impact on victims” as well as severe distress and other strong emotions and physical  
 15 reactions.

16           48. Individuals are particularly concerned with protecting the privacy of  
 17 their financial account information and social security numbers. Neal O’Farrell, a  
 18 security and identity theft expert for Credit Sesame, calls a Social Security number  
 19 “your secret sauce,” that is “as good as your DNA to hackers.” There are long-term  
 20

21 \_\_\_\_\_  
 22 <sup>16</sup> *Annual Number of Data Breaches and Exposed Records in the United States from*  
 23 *2005 to 2020*, Statista, [https://www.statista.com/statistics/273550/data-breaches-](https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed)  
 24 [recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed](https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed) (last  
 25 accessed July 20, 2022).

26 <sup>17</sup> *Id.*

27 <sup>18</sup> See Brian Stack, *Here’s How Much Your Personal Information is Selling for on the*  
 28 *Dark Web*, Experian (Dec. 6, 2017), available at:  
[https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web)  
[information-is-selling-for-on-the-dark-web.](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web)

1 consequences to data breach victims whose social security numbers are taken and  
2 used by hackers. Even if they know their social security numbers have been accessed,  
3 Plaintiffs and Class members cannot obtain new numbers unless they become a victim  
4 of Social Security number misuse. Even then, the Social Security Administration has  
5 warned that “a new number probably won’t solve all [] problems . . . and won’t  
6 guarantee . . . a fresh start.”

7       49. Data breaches involving medical and health information, like the one  
8 here at issue, amplify those risks considerably because of the access it provides to  
9 criminals.

10       50. When the PII includes medical information, the identity theft could  
11 extend to sending the victim fake medical bills or obtaining medical services using  
12 the victim’s insurance or financial information, which can result in unknown, unpaid  
13 bills being sent to collections or using the victim’s health insurance.<sup>19</sup>

14       51. Moreover, unlike victims of just credit card identity theft, victims of  
15 medical records data breaches cannot simply “reverse” fraudulent transactions.<sup>20</sup> As  
16 such, victims of data breaches in which hackers misappropriate highly sensitive  
17 patient PII often are unable to recover the losses they suffer as a result thereof, and  
18 must expend additional time and money to mitigate and protect themselves from  
19 further attempts at identity theft. One study found that the majority of medical identity  
20 theft victims had to pay an average of \$13,500 to resolve issues stemming from the  
21  
22

---

23 <sup>19</sup> Medical Identity Theft, Federal Trade Commission (Jan. 2011), available at:  
24 [https://www.bulkorder.ftc.gov/system/files/publications/bus75-medical-identity-](https://www.bulkorder.ftc.gov/system/files/publications/bus75-medical-identity-theft-faq-health-care-health-plan.pdf)  
25 [theft-faq-health-care-health-plan.pdf](https://www.bulkorder.ftc.gov/system/files/publications/bus75-medical-identity-theft-faq-health-care-health-plan.pdf).

26 <sup>20</sup> See *The \$300 Billion Attack: The Revenue Risk and Human Impact of Healthcare*  
27 *Provider Cyber Security Inaction*, Accenture, available at:  
28 [https://www.accenture.com/\\_acnmedia/PDF-54/Accenture-Health-Cybersecurity-](https://www.accenture.com/_acnmedia/PDF-54/Accenture-Health-Cybersecurity-300-Billion-at-Risk.pdf)  
[300-Billion-at-Risk.pdf](https://www.accenture.com/_acnmedia/PDF-54/Accenture-Health-Cybersecurity-300-Billion-at-Risk.pdf) (last visited Feb. 12, 2021).

1 data breach, and only 10% of victims achieve a completely satisfactory resolution.<sup>21</sup>  
 2 Almost one-third of medical identity theft victims lost their health insurance as a result  
 3 of the identity theft.<sup>22</sup>

4 52. As explained by Kunal Rupani, director of product management at  
 5 Accellion, a private cloud solutions company, in the context of a different medical  
 6 data breach:

7 Unlike credit card numbers and other financial data, healthcare  
 8 information doesn't have an expiration date. As a result, a patient's  
 9 records can sell on the black market for upwards of fifty times the  
 10 amount of their credit card number, making hospitals and other  
 healthcare organizations extremely lucrative targets for cybercriminals.<sup>23</sup>

11 53. SecureWorks, a division of Dell Inc., echoed that sentiment, noting that  
 12 "[i]t's a well known truism within much of the healthcare data security community  
 13 that an individual healthcare record is worth more on the black market (\$50, on  
 14 average) than a U.S.-based credit card and personal identity with social security  
 15 number combined."<sup>24</sup> The reason is that thieves "[c]an use a healthcare record to  
 16 submit false medical claims (and thus obtain free medical care), purchase prescription  
 17  
 18  
 19

20 <sup>21</sup> See *Fifth Annual Study on Medical Identity Theft*, Ponemon Institute LLC (Feb.  
 21 2015), at pp.2, 7, available at:  
[https://static.nationwide.com/static/2014\\_Medical\\_ID\\_Theft\\_Study.pdf?r=65](https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65).

22 <sup>22</sup> *Id.*

23 <sup>23</sup> Jeff Goldman, 21st Century Oncology Notifies 2.2 Million Patients of Data Breach  
 24 (Mar. 11, 2016), [http://www.esecurityplanet.com/network-security/21st-century-](http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html)  
 25 [oncology-notifies-2.2-million-patients-of-data-breach.html](http://www.esecurityplanet.com/network-security/21st-century-oncology-notifies-2.2-million-patients-of-data-breach.html) (last visited Feb. 11,  
 2021).

26 <sup>24</sup> What's the Market Value of a Healthcare Record, Dell SecureWorks (Dec. 13,  
 27 2012), [https://www.secureworks.com/blog/general-market-value-of-a-healthcare-](https://www.secureworks.com/blog/general-market-value-of-a-healthcare-record)  
 28 [record](https://www.secureworks.com/blog/general-market-value-of-a-healthcare-record) (last visited Feb. 11, 2021).



1 medication, or resell the record on the black market.”<sup>25</sup>

2 54. Similarly, the FBI Cyber Division in an April 8, 2014 Private Industry  
3 Notification, advised:

4 Cyber criminals are selling [medical] information on the black market at  
5 a rate of \$50 for each partial EHR, compared to \$1 for a stolen social  
6 security number or credit card number. EHR can then be used to file  
7 fraudulent insurance claims, obtain prescription medication, and  
8 advance identity theft. EHR theft is also more difficult to detect, taking  
almost twice as long as normal identity theft.<sup>26</sup>

9 55. In light of the dozens of high-profile health and medical information data  
10 breaches that have been reported in recent years, entities like Defendants that are  
11 charged with maintaining and securing patient PII know the importance of protecting  
12 that information from unauthorized disclosure. Indeed, on information and belief,  
13 Defendants were aware of highly publicized security breaches where PII and  
14 protected health information was accessed by unauthorized cybercriminals, including  
15 breaches of computer systems involving: UnityPoint Health, Lifetime Healthcare,  
16 Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premiera  
17 Blue Cross, and many others.<sup>27</sup>

18 56. In addition, the Federal Trade Commission (“FTC”) has brought dozens  
19 of cases against companies that have engaged in unfair or deceptive practices  
20 involving inadequate protection of consumers’ personal data, including recent cases  
21 concerning health-related information against LabMD, Inc., SkyMed International,

---

22 <sup>25</sup> *Id.*

23  
24 <sup>26</sup> Federal Bureau of Investigation, FBI Cyber Division Private Industry Notification  
25 (Apr. 8, 2014), <https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf> (last visited Feb. 11, 2021).

26 <sup>27</sup> See e.g., *Healthcare Data Breach Statistics*, HIPAA Journal, available at:  
27 <https://www.hipaajournal.com/healthcare-data-breach-statistics> (last accessed Feb.  
28 15, 2021).

1 Inc., and others. The FTC publicized these enforcement actions to place companies  
2 like Defendants on notice of their obligation to safeguard customer and patient  
3 information.

4 57. Indeed, cyberattacks have become so notorious that the FBI and U.S.  
5 Secret Service have issued a warning to potential targets so they are aware of and take  
6 appropriate measures to prepare for and are able to thwart such an attack.

7 58. Further, consumers' PII remains of high value to criminals, as evidenced  
8 by the prices they will pay through the dark web. Numerous sources cite dark web  
9 pricing for stolen identity credentials. For example, personal information can be sold  
10 at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to  
11 \$200.<sup>28</sup> According to the Dark Web Price Index for 2021, payment card details for an  
12 account balance up to \$1,000 have an average market value of \$150, credit card details  
13 with an account balance up to \$5,000 have an average market value of \$240, stolen  
14 online banking logins with a minimum of \$100 on the account have an average market  
15 value of \$40, and stolen online banking logins with a minimum of \$2,000 on the  
16 account have an average market value of \$120.<sup>29</sup>

17 59. Social Security numbers are among the most dangerous kind of personal  
18 information to have stolen because they may be put to a variety of fraudulent uses and  
19 are difficult for an individual to change. The Social Security Administration stresses  
20 that the loss of an individual's Social Security number, as is the case here, can lead to  
21 identity theft and extensive financial fraud:

22  
23  
24 <sup>28</sup> *Your personal data is for sale on the dark web. Here's how much it costs*, Digital  
25 Trends, Oct. 16, 2019, available at:  
26 <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 20, 2022).

27 <sup>29</sup> Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFFAIRS (Dec. 10, 2021),  
28 available at <https://www.privacyaffairs.com/dark-web-price-index-2021/>.

1 A dishonest person who has your Social Security number can use it to  
2 get other personal information about you. Identity thieves can use your  
3 number and your good credit to apply for more credit in your name.  
4 Then, they use the credit cards and don't pay the bills, it damages your  
5 credit. You may not find out that someone is using your number until  
6 you're turned down for credit, or you begin to get calls from unknown  
7 creditors demanding payment for items you never bought. Someone  
8 illegally using your Social Security number and assuming your identity  
9 can cause a lot of problems.<sup>30</sup>

10 60. Furthermore, trying to change or cancel a stolen Social Security number  
11 is no minor task. An individual cannot obtain a new Social Security number without  
12 significant paperwork and evidence of actual misuse. In other words, preventive  
13 action to defend against the possibility of misuse of a Social Security number is not  
14 permitted; an individual must show evidence of actual, ongoing fraud activity to  
15 obtain a new number.

16 61. Even then, a new Social Security number may not be effective, as "[t]he  
17 credit bureaus and banks are able to link the new number very quickly to the old  
18 number, so all of that old bad information is quickly inherited into the new Social  
19 Security number."<sup>31</sup>

20 62. This data, as one would expect, demands a much higher price on the  
21 black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained,  
22 "[c]ompared to credit card information, personally identifiable information and Social  
23

---

24 <sup>30</sup> *Identity Theft and Your Social Security Number*, SOCIAL SECURITY  
25 ADMINISTRATION (July 2021), available at <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

26 <sup>31</sup> Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce*  
27 *Back*, NPR (Feb. 9, 2015), available at  
28 <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

1 Security Numbers are worth more than 10x on the black market.”<sup>32</sup>

2 63. Given the nature of Defendants’ Data Breach, as well as the long delay  
3 in notification to the Class, it is foreseeable that the compromised PII has been or will  
4 be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the  
5 cybercriminals who possess Plaintiffs’ and Class members’ PII can easily obtain  
6 Plaintiffs’ and Class members’ tax returns or open fraudulent credit card accounts in  
7 Class members’ names.

8 64. Based on the foregoing, the information compromised in the Data Breach  
9 is significantly more valuable than the loss of, for example, credit card information in  
10 a retailer data breach, because credit card victims can cancel or close credit and debit  
11 card accounts.<sup>33</sup> The information compromised in this Data Breach is impossible to  
12 “close” and difficult, if not impossible, to change.

13 65. To date, Defendants has offered its consumers *only one year* of identity  
14 monitoring services. The offered services are inadequate to protect Plaintiffs and the  
15 Class from the threats they face for years to come, particularly in light of the PII at  
16 issue here.

17 66. Despite the prevalence of public announcements of data breach and data  
18 security compromises, its own acknowledgment of the risks posed by data breaches,  
19 and its own acknowledgment of its duties to keep PII private and secure, Defendants  
20 failed to take appropriate steps to protect the PII of Plaintiffs and the Class from  
21 misappropriation. As a result, the injuries to Plaintiffs and the Class were directly and

---

22 <sup>32</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen*  
23 *Credit Card Numbers*, COMPUTER WORLD (Feb. 6, 2015), available at  
24 [http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-](http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html)  
25 [for-10x-price-of-stolen-credit-card-numbers.html](http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html).

26 <sup>33</sup> See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New*  
27 *Report Finds*, FORBES (Mar. 25, 2020), available at  
28 [https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-](https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1)  
[number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1](https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1).

1 proximately caused by Defendants' failure to implement or maintain adequate data  
2 security measures for its current and former patients.

3 **E. Defendants Had a Duty and Obligation to Protect PII**

4 67. Defendants has an obligation, both statutory and self-imposed, to keep  
5 confidential and protect from unauthorized access and/or disclosure Plaintiffs' and  
6 Class members' PII. Defendants' obligations are derived from: 1) government  
7 regulations and state laws, including HIPAA and FTC rules and regulations; 2)  
8 industry standards; and 3) promises and representations regarding the handling of  
9 sensitive PII and medical records. Plaintiffs and Class members provided, and  
10 Defendants obtained, their PII on the understanding that their PII would be protected  
11 and safeguarded from unauthorized access or disclosure.

12 68. HIPAA requires, *inter alia*, that Covered Entities and Business  
13 Associates implement and maintain policies, procedures, systems and safeguards that  
14 ensure the confidentiality and integrity of consumer and patient PII, protect against  
15 any reasonably anticipated threats or hazards to the security or integrity of consumer  
16 and patient PII, regularly review access to data bases containing protected  
17 information, and procedures and systems to detect, contain, and correct any  
18 unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

19 69. Additionally, HIPAA requires Covered Entities and Business Associates  
20 to provide notification to every affected individual following the impermissible use  
21 or disclosures of any protected health information. The individual notice must be  
22 provided to affected individuals without unreasonable delay and no later than 60 days  
23 following discovery of the breach. Further, for a breach involving more than 500  
24 individuals, entities are required to provide notice in prominent media outlets. *See* 45  
25 CFR § 164.400, *et seq.*

26 70. Defendants represent to patients and customers that they will comply  
27 with HIPAA requirements concerning the protection of PII and protected health  
28

1 information and prompt and adequate notification of data breaches.<sup>34</sup>

2 71. Additionally, the Federal Trade Commission's ("FTC") Health Breach  
3 Notification Rule obligates companies that suffered a data breach to provide notice to  
4 every individual affected by the data breach, as well as notifying the media and the  
5 FTC. *See* 16 CFR 318.1, *et seq.*

6 72. The FTC defines identity theft as "a fraud committed or attempted using  
7 the identifying information of another person without authority."<sup>35</sup> The FTC describes  
8 "identifying information" as "any name or number that may be used, alone or in  
9 conjunction with any other information, to identify a specific person," including,  
10 among other things, "[n]ame, Social Security number, date of birth, official State or  
11 government issued driver's license or identification number, alien registration  
12 number, government passport number, employer or taxpayer identification  
13 number."<sup>36</sup>

14 73. The FTC has issued numerous guides for businesses highlighting the  
15 importance of reasonable data security practices. According to the FTC, the need for  
16 data security should be factored into all business decision-making.<sup>37</sup>

17 74. In 2016, the FTC updated its publication, *Protecting Personal*  
18 *Information: A Guide for Business*, which established guidelines for fundamental data  
19  
20  
21

---

22 <sup>34</sup> *See, e.g., Notice of Privacy Practices*, Regal Medical Group,  
23 <https://www.regalmed.com/privacy-notice/> (last accessed Feb. 24, 2023).

24 <sup>35</sup> 17 C.F.R. § 248.201.

25 <sup>36</sup> *Id.*

26 <sup>37</sup> *Start With Security*, Federal Trade Commission (June 2015), available at  
27 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf)  
28 [startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf).

1 security principles and practices for business.<sup>38</sup> The guidelines note businesses should  
 2 protect the personal information that they keep; properly dispose of personal  
 3 information that is no longer needed; encrypt information stored on computer  
 4 networks; understand their network's vulnerabilities; and implement policies to  
 5 correct security problems.<sup>39</sup> The guidelines also recommend that businesses use an  
 6 intrusion detection system to expose a breach as soon as it occurs; monitor all  
 7 incoming traffic for activity indicating someone is attempting to hack the system;  
 8 watch for large amounts of data being transmitted from the system; and have a  
 9 response plan ready in the event of a breach.<sup>40</sup> Defendants clearly failed to do any of  
 10 the foregoing, as evidenced by the length of the Data Breach, and the amount of data  
 11 exfiltrated.

12 75. Here, at all relevant times, Defendants were fully aware of their  
 13 obligation to protect the PII and protected health information of their current and  
 14 former patients, including Plaintiffs and the Class, and Defendants are sophisticated  
 15 and technologically savvy medical treatment centers that rely extensively on  
 16 technology systems and networks to maintain their medical practice, including  
 17 transmitting their patients' PII, protected health information, and medical information  
 18 in order to operate their business.<sup>41</sup>

19 \_\_\_\_\_  
 20 <sup>38</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n  
 21 (Jan. 23, 2015), available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

22 <sup>39</sup> *Id.*

23 <sup>40</sup> *Id.*

24 <sup>41</sup> *Submitted Breach Notification Sample*, Office of the Attorney General California  
 25 Department of Justice,  
 26 <https://oag.ca.gov/system/files/Regal%20John%20Doe%20Letter%20Feb%201%202023.pdf> (last accessed Feb. 22, 2023); *HIPAA Policies and Practices*, Regal Medical  
 27 Group, <https://www.regalmed.com/compliance-and-resources/hipaa-policies-and-procedures/> (last accessed Feb. 24, 2023).  
 28



1        76. Defendants had, and continue to have, a duty to exercise reasonable care  
2 in collecting, storing, and protecting the PII and medical information from the  
3 foreseeable risk of a data breach. The duty arises out of the special relationship that  
4 exists between Defendants, and Plaintiffs and Class members. Defendants alone had  
5 the exclusive ability to implement adequate security measures to their cyber security  
6 network to secure and protect Plaintiffs' and Class members' PII.

7        77. Defendants' failure to follow the FTC guidelines and their subsequent  
8 failure to employ reasonable and appropriate measures to protect against unauthorized  
9 access to confidential data constitutes unfair acts or practices prohibited by Section 5  
10 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

11        78. Further, Defendants had a duty to promptly notify Plaintiffs and the  
12 Class that their PII was accessed by unauthorized persons.

13 **F. Defendants Violated HIPAA, FTC and Industry Standard Data Protection**  
14 **Protocols**

15        79. HIPAA obligates Covered Entities and Business Associates to adopt  
16 administrative, physical, and technology safeguards to ensure the confidentiality,  
17 integrity, and security of consumer and patient PII.

18        80. The FTC rules, regulations, and guidelines obligate businesses to protect  
19 PII, from unauthorized access or disclosure by unauthorized persons.

20        81. At all relevant times, Defendants were fully aware of their obligation to  
21 protect the customers and patient PII because it is a sophisticated business entity that  
22 is in the business of maintaining and transmitting PII, including personal health and  
23 medical records.

24        82. Defendants were also aware of the significant consequences of their  
25 failure to protect PII for the hundreds of thousands of patients who provided their PII  
26 and medical information to Defendants, and knew that this data, if hacked, would  
27 injure consumers, including Plaintiffs and Class members.

28        83. Unfortunately, Defendants failed to comply with HIPAA, FTC rules,

1 regulations and guidelines, and industry standards concerning the protection and  
2 security of PII. As evidenced by the duration, scope, and nature of the Data Breach,  
3 among its many deficient practices, Defendants failed in, *inter alia*, the following  
4 respects:

- 5 a. Developing and employing adequate intrusion detection systems;
- 6 b. Engaging in regular reviews of audit logs and authentication records;
- 7 c. Developing and maintaining adequate data security systems to reduce  
8 the risk of data breaches and cyberattacks;
- 9 d. Ensuring the confidentiality and integrity of current and former  
10 patients' PII, including protected health and information and records  
11 that Defendants receive and maintain;
- 12 e. Protecting against any reasonably anticipated threats or hazards to the  
13 security or integrity of its current and former patients' PII;
- 14 f. Implementing policies and procedures to prevent, detect, contain, and  
15 correct security violations;
- 16 g. Developing adequate policies and procedures to regularly review  
17 records of system activity, such as audit logs, access reports, and  
18 security incident tracking reports;
- 19 h. Implementing technical policies, procedures and safeguards for  
20 electronically stored information concerning PII that permit access for  
21 only those persons or programs that have specifically been granted  
22 access; and
- 23 i. Other similar measures to protect the security and confidentiality of  
24 its current and former patients' PII.

25 84. Had Defendants implemented the above-described data security  
26 protocols, policies, and/or procedures, the consequences of the Data Breach could  
27 have been avoided or greatly reduced. Defendants could have prevented or detected  
28 the Data Breach prior to the hackers accessing Defendants' systems and extracting

1 sensitive and personal information; the amount and/or types of PII accessed by the  
2 hackers could have been avoided or greatly reduced; and current and former patients  
3 of Defendants would have been notified sooner, allowing them to promptly take  
4 protective and mitigating actions.

5 **G. Defendants' Data Security Practices are Inadequate and Inconsistent with**  
6 **its Self-Imposed Data Security Obligations**

7 85. Defendants purport to care about data security and safeguarding patients'  
8 PII, and represents that they will keep secure and confidential the PII belonging to  
9 their current and former patients.

10 86. Plaintiffs' and Class members' PII and medical information was  
11 provided to Defendants in reliance on its promises and self-imposed obligations to  
12 keep PII and medical information confidential, and to secure the PII and medical  
13 information from unauthorized access by malevolent actors. Defendants failed to do  
14 so.

15 87. The length of the Data Breach also demonstrates that Defendants failed  
16 to safeguard PII by, *inter alia*: maintaining an adequate data security environment to  
17 reduce the risk of a data breach; periodically auditing its security systems to discover  
18 intrusions like the Data Breach; and retaining outside vendors to periodically test its  
19 network, servers, systems and workstations.

20 88. Had Defendants undertaken the actions that federal and state law require,  
21 the Data Breach could have been prevented or the consequences of the Data Breach  
22 significantly reduced, as Defendants would have detected the Data Breach prior to the  
23 hackers extracting data from Defendants' networks, and Defendants' current and  
24 former patients would have been notified of the Data Breach sooner, allowing them  
25 to take necessary protective or mitigating measures much earlier.

26 89. Indeed, following the Data Breach, Defendants effectively conceded that  
27 its security practices were inadequate and ineffective. In the Notice it sent to Plaintiffs  
28 and others, Defendants acknowledged that the Data Breach required it to "hire[] third-

1 party vendors experienced in this area to assist with our response to the incident” See  
2 Exhibit A.

### 3 **H. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach**

4 90. Like any data hack, the Data Breach presents major problems for all  
5 affected. According to Jonathan Bowers, a fraud and data specialist at fraud  
6 prevention provider Trustev, “Give a fraudster your comprehensive personal  
7 information, they can steal your identity and take out lines of credit that destroy your  
8 finances for years to come.”<sup>42</sup>

9 91. The FTC warns the public to pay particular attention to how they keep  
10 personally identifying information including Social Security numbers and other  
11 sensitive data. As the FTC notes, “once identity thieves have your personal  
12 information, they can drain your bank account, run up charges on your credit cards,  
13 open new utility accounts, or get medical treatment on your health insurance.”<sup>43</sup>

14 92. The ramifications of Defendants’ failure to properly secure PII,  
15 including Plaintiffs’ and Class members’ PII, are severe. Identity theft occurs when  
16 someone uses another person’s financial, and personal information, such as that  
17 person’s name, address, Social Security number, and other information, without  
18 permission to commit fraud or other crimes.

19 93. According to data security experts, one out of every four data breach  
20 notification recipients becomes a victim of identity fraud.

21 94. Furthermore, PII has a long shelf-life because it contains different forms  
22 of personal information, it can be used in more ways than one, and it typically takes  
23

---

24 <sup>42</sup> Roger Cheng, *Data Breach Hits Roughly 15M T-Mobile Customers, Applicants*,  
25 CNET (Oct. 1, 2015), available at: <http://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/>. (last accessed July 20, 2022).

26 <sup>43</sup> *Warning Signs of Identity Theft*, Federal Trade Comm’n, available at  
27 <https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft> (last accessed July  
28 20, 2022).

1 time for an information breach to be detected.

2 95. Accordingly, Defendants' wrongful actions and/or inaction and the  
3 resulting Data Breach have also placed Plaintiffs and the Class at an imminent,  
4 immediate, and continuing increased risk of identity theft and identity fraud.<sup>44</sup> Indeed,  
5 "[t]he level of risk is growing for anyone whose information is stolen in a data  
6 breach."<sup>45</sup> Javelin Strategy & Research, a leading provider of quantitative and  
7 qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial  
8 risk of fraud."<sup>46</sup> Moreover, there is a high likelihood that significant identity fraud  
9 and/or identity theft has not yet been discovered or reported. Even data that have not  
10 yet been exploited by cybercriminals bears a high risk that the cybercriminals who  
11 now possess Class members' PII will do so at a later date or re-sell it.

12 96. In response to the Data Breach, Defendants offered to provide certain  
13 individuals whose PII was exposed in the Data Breach with one year of credit  
14 monitoring. However, one year of complimentary credit monitoring is a time frame  
15 much shorter than what is necessary to protect against the lifelong risk of harm  
16 imposed on Plaintiffs and Class members by Defendants' failures.

17 97. Moreover, the credit monitoring offered by Defendants is inadequate to  
18 protect Plaintiffs and Class members from the injuries resulting from the unauthorized  
19

20 <sup>44</sup> *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE  
21 INFORMATION INSTITUTE BLOG (February 23, 2012), available at  
22 <http://www.iii.org/insuranceindustryblog/?p=267>.

23 <sup>45</sup> Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July  
24 23, 2014), available at <http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php>.

25 <sup>46</sup> *The Consumer Data Insecurity Report: Examining The Data Breach- Identity*  
26 *Fraud Paradigm In Four Major Metropolitan Areas*, NORTHWESTERN UNIVERSITY,  
27 available at [https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport\\_byN](https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf)  
28 [CL.pdf](https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf).

1 access and exfiltration of their sensitive PII.

2 98. Here, due to the Breach, Plaintiffs and Class members have been exposed  
3 to injuries that include, but are not limited to:

- 4 a. Theft of PII, including protected health information;
- 5 b. Costs associated with the detection and prevention of identity theft and  
6 unauthorized use of financial accounts as a direct and proximate result  
7 of the PII stolen during the Data Breach;
- 8 c. Damages arising from the inability to use accounts that may have been  
9 compromised during the Data Breach;
- 10 d. Costs associated with spending time to address and mitigate the actual  
11 and future consequences of the Data Breach, such as finding  
12 fraudulent charges, cancelling and reissuing payment cards,  
13 purchasing credit monitoring and identity theft protection services,  
14 placing freezes and alerts on their credit reports, contacting their  
15 financial institutions to notify them that their personal information was  
16 exposed and to dispute fraudulent charges, imposition of withdrawal  
17 and purchase limits on compromised accounts, including but not  
18 limited to lost productivity and opportunities, time taken from the  
19 enjoyment of one's life, and the inconvenience, nuisance, and  
20 annoyance of dealing with all issues resulting from the Data Breach,  
21 if they were fortunate enough to learn of the Data Breach despite  
22 Defendants' delay in disseminating notice in accordance with state  
23 law;
- 24 e. The imminent and impending injury resulting from potential fraud and  
25 identity theft posed because their PII is exposed for theft and sale on  
26 the dark web; and
- 27 f. The loss of Plaintiffs' and Class members' privacy.

28 99. Plaintiffs and Class members have suffered imminent and impending

1 injury arising from the substantially increased risk of fraud, identity theft, and misuse  
 2 resulting from their PII and protected health information being accessed by  
 3 cybercriminals, risks that will not abate within a mere one year: the unauthorized  
 4 access of Plaintiffs' and Class members' PII, especially their Social Security numbers,  
 5 puts Plaintiffs and the Class at risk of identity theft indefinitely, and well beyond the  
 6 limited period of credit monitoring that Defendants offered victims of the Breach. The  
 7 one year of credit monitoring that Defendants offered to certain victims of the Data  
 8 Breach is inadequate to mitigate the aforementioned injuries Plaintiffs and Class  
 9 members have suffered and will continue to suffer as a result of the Data Breach.

10 100. As a direct and proximate result of Defendants' acts and omissions in  
 11 failing to protect and secure PII and medical information, Plaintiffs and Class  
 12 members have been placed at a substantial risk of harm in the form of identity theft,  
 13 and have incurred and will incur actual damages in an attempt to prevent identity theft.

14 101. Plaintiffs retain an interest in ensuring there are no future breaches, in  
 15 addition to seeking a remedy for the harms suffered as a result of the Data Breach on  
 16 behalf of both themselves and similarly situated individuals whose PII and medical  
 17 information was accessed in the Data Breach.

18 102. Defendants are aware of the ongoing harm that the Data Breach has and  
 19 will continue to impose on Defendants' current and former patients, as the notices that  
 20 it posted and sent to Plaintiffs and Class members regarding the Data Breach advise  
 21 the victims to "take immediate steps to protect themselves from potential harm[.]" *See*  
 22 Exhibit A.

### 23 **I. The Downs Plaintiffs' Experience**

24 103. In February 2023, both Plaintiffs received notices from Defendants that  
 25 each of their PII and medical treatment and health information had been improperly  
 26 accessed and/or obtained by third parties. Each notice indicated that Plaintiffs' PII,  
 27 inclusive of their Social Security numbers, dates of birth, full names, addresses,  
 28 telephone numbers, information regarding medical treatment and diagnosis,



1 prescription data, laboratory test results, radiology reports, and health plan member  
2 numbers, were compromised in the Data Breach.

3 104. As a result of the Data Breach, Plaintiffs have made reasonable efforts  
4 to mitigate the impact of the Data Breach, including, but not limited to, researching  
5 the Data Breach; reviewing credit reports and financial account statements for any  
6 indications of actual or attempted identity theft or fraud; and researching credit  
7 monitoring and identity theft protection services. Plaintiffs have spent several hours  
8 dealing with the Data Breach, valuable time Plaintiffs otherwise would have spent on  
9 other activities, including, but not limited to, work and/or recreation.

10 105. Between December 2022 and February 2023, Plaintiff Shannon Masser  
11 Downs has received multiple notices that fraudulent activity is occurring within her  
12 authorized accounts. The notices included an alert that an unknown user attempted to  
13 register for a credit card in her name and that her Social Security Number had been  
14 breached.

15 106. As a result of the Data Breach, Plaintiffs have suffered anxiety as a result  
16 of the release of their PII, which they believed would be protected from unauthorized  
17 access and disclosure, including anxiety about unauthorized parties viewing, selling,  
18 and/or using their PII for purposes of identity theft and fraud. Plaintiffs are concerned  
19 about identity theft and fraud, as well as the consequences of such identity theft and  
20 fraud resulting from the Data Breach.

21 107. Plaintiffs suffered actual injury from having their PII compromised as a  
22 result of the Data Breach including, but not limited to (a) damage to and diminution  
23 in the value of their PII, a form of property that Defendants obtained from Plaintiff;  
24 (b) violation of their privacy rights; and (c) present, imminent and impending injury  
25 arising from the increased risk of identity theft and fraud.

26 108. As a result of the Data Breach, Plaintiffs anticipate spending  
27 considerable time and money on an ongoing basis to try to mitigate and address harms  
28 caused by the Data Breach. As a result of the Data Breach, Plaintiffs are at a present

1 risk and will continue to be at increased risk of identity theft and fraud for years to  
2 come.

3 **J. Plaintiff Hinestrosa's Experience**

4 109. In February 2023, Plaintiff Hinestrosa received a notice from Defendants  
5 that her PII and medical information had been improperly accessed and/or obtained  
6 by third parties. This notice indicated that Plaintiff Hinestrosa's PII, inclusive of her  
7 Social Security number, date of birth, full name, address, telephone number,  
8 information regarding medical treatment and diagnosis, prescription data, laboratory  
9 test results, radiology reports, and health plan member number, were compromised in  
10 the Data Breach.

11 110. As a result of the Data Breach, Plaintiff Hinestrosa has made reasonable  
12 efforts to mitigate the impact of the Data Breach, including, but not limited to,  
13 researching the Data Breach; reviewing credit reports and financial account  
14 statements for any indications of actual or attempted identity theft or fraud; and  
15 researching credit monitoring and identity theft protection services. Plaintiff  
16 Hinestrosa has spent several hours dealing with the Data Breach, valuable time  
17 Plaintiff Hinestrosa otherwise would have spent on other activities, including, but not  
18 limited to, work and/or recreation.

19 111. In December of 2022, Plaintiff Hinestrosa received notice that an  
20 unauthorized actor had attempted to access her credit card. Additionally, in February  
21 of 2023, Plaintiff Hinestrosa received a notice from Citibank of fraudulent activity on  
22 her bank account, and, as a result, Citibank canceled her debit card and de-activated  
23 her account.

24 112. As a result of the Data Breach, Plaintiff Hinestrosa has suffered anxiety  
25 as a result of the release of her PII, which she believed would be protected from  
26 unauthorized access and disclosure, including anxiety about unauthorized parties  
27 viewing, selling, and/or using her PII for purposes of identity theft and fraud. Plaintiff  
28 Hinestrosa is concerned about identity theft and fraud, as well as the consequences of

1 such identity theft and fraud resulting from the Data Breach.

2 113. Plaintiff Hinestrota suffered actual injury from having her PII  
3 compromised as a result of the Data Breach including, but not limited to (a) damage  
4 to and diminution in the value of her PII, a form of property that Defendants obtained  
5 from Plaintiff; (b) violation of her privacy rights; and (c) present, imminent and  
6 impending injury arising from the increased risk of identity theft and fraud.

7 114. As a result of the Data Breach, Plaintiff Hinestrota anticipates spending  
8 considerable time and money on an ongoing basis to try to mitigate and address harms  
9 caused by the Data Breach. As a result of the Data Breach, Plaintiff Hinestrota is at a  
10 present risk and will continue to be at increased risk of identity theft and fraud for  
11 years to come.

### 12 **CLASS ALLEGATIONS**

13 115. Plaintiffs bring this action on behalf of themselves and, pursuant to Fed.  
14 R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

15 All persons in the United States whose PII was accessed in the Data  
16 Breach.

17 Excluded from the Class are Defendants, their executives and officers, and the  
18 Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change or expand  
19 the Class definition after conducting discovery.

20 116. In the alternative, Plaintiffs bring this action on behalf of themselves and,  
21 pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

22 All persons who are residents of the State of California whose PII was  
23 accessed in the Data Breach (the "California Subclass").

24 Excluded from the California Subclass are Defendants, their executives and officers,  
25 and the Judge(s) assigned to this case.

26 117. Numerosity: Upon information and belief, the Class is so numerous that  
27 joinder of all members is impracticable. While the exact number and identities of  
28 individual members of the Class are unknown at this time, such information being in

1 the sole possession of Defendants and obtainable by Plaintiffs only through the  
2 discovery process, Plaintiffs believe, and on that basis allege, that approximately  
3 3,300,638 individuals comprise the Class and were affected by the Data Breach. The  
4 members of the Class will be identifiable through information and records in  
5 Defendants' possession, custody, and control.

6 118. Existence and Predominance of Common Questions of Fact and Law:  
7 Common questions of law and fact exist as to all members of the Class. These  
8 questions predominate over the questions affecting individual Class members. These  
9 common legal and factual questions include, but are not limited to:

- 10 a. Whether Defendants' data security and retention policies were  
11 unreasonable;
- 12 b. Whether Defendants failed to protect the confidential and highly  
13 sensitive information with which it was entrusted;
- 14 c. Whether Defendants owed a duty to Plaintiffs and Class members to  
15 safeguard their PII;
- 16 d. Whether Defendants breached any legal duties in connection with the  
17 Data Breach;
- 18 e. Whether Defendants' conduct was intentional, reckless, willful or  
19 negligent;
- 20 f. Whether an implied contract was created concerning the security of  
21 Plaintiffs' and Class members' PII;
- 22 g. Whether Defendants breached that implied contract by failing to  
23 protect and keep secure Plaintiffs' and Class members' PII and/or  
24 failing to timely and adequately notify Plaintiffs and Class members  
25 of the Data Breach;
- 26 h. Whether Plaintiffs and Class members suffered damages as a result of  
27 Defendants' conduct; and
- 28 i. Whether Plaintiffs and the Class are entitled to monetary damages,

1           injunctive relief and/or other remedies and, if so, the nature of any  
2           such relief.

3           119. Typicality: All of Plaintiffs' claims are typical of the claims of the Class  
4 since Plaintiffs and all members of the Class had their PII compromised in the Data  
5 Breach. Plaintiffs and the members of the Class sustained damages as a result of  
6 Defendants' uniform wrongful conduct.

7           120. Adequacy: Plaintiffs are adequate representatives because their interests  
8 do not materially or irreconcilably conflict with the interests of the Class they seek to  
9 represent, they have retained counsel competent and highly experienced in complex  
10 class action litigation, and intend to prosecute this action vigorously. Plaintiffs and  
11 their counsel will fairly and adequately protect the interests of the Class. Neither  
12 Plaintiffs nor their counsel have any interests that are antagonistic to the interests of  
13 other members of the Class.

14           121. Superiority: A class action is superior to all other available means of fair  
15 and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered  
16 by each individual Class member is relatively small in comparison to the burden and  
17 expense of individual prosecution of the complex and extensive litigation necessitated  
18 by Defendants' conduct. It would be virtually impossible for members of the Class  
19 individually to effectively redress the wrongs done to them. Even if the members of  
20 the Class could afford such individual litigation, the court system could not.  
21 Individualized litigation presents a potential for inconsistent or contradictory  
22 judgments. Individualized litigation increases the delay and expense to all parties and  
23 to the court system presented by the complex legal and factual issues of the case. By  
24 contrast, the class action device presents far fewer management difficulties, and  
25 provides the benefits of single adjudication, economy of scale, and comprehensive  
26 supervision by a single court. Members of the Class can be readily identified and  
27 notified based on, *inter alia*, Defendants records and databases.

28           122. Defendants have acted, and refused to act, on grounds generally

1 applicable to the Class, thereby making appropriate final relief with respect to the  
2 Class as a whole.

3 **CAUSES OF ACTION**

4 **COUNT I — Negligence**

5 **(By Plaintiffs on behalf of the Class, or, in the alternative, the California  
6 Subclass)**

7 123. Plaintiffs incorporate and reallege all allegations above as if fully set  
8 forth herein.

9 124. This count is brought on behalf of all Class members.

10 125. Defendants owed a duty to Plaintiffs and the Class to use and exercise  
11 reasonable and due care in obtaining, retaining, and securing the PII that Defendants  
12 collected.

13 126. Defendants owed a duty to Plaintiffs and the Class to provide security,  
14 consistent with industry standards and requirements, and to ensure that its cyber  
15 networks and systems, and the personnel responsible for them, adequately protected  
16 the PII that Defendants collected.

17 127. Defendants owed a duty to Plaintiffs and the Class to implement  
18 processes to quickly detect a data breach, to timely act on warnings about data  
19 breaches, and to inform the victims of a data breach as soon as possible after it is  
20 discovered.

21 128. Defendants owed a duty of care to Plaintiffs and the Class because they  
22 were a foreseeable and probable victim of any inadequate data security practices.

23 129. Defendants solicited, gathered, and stored the PII belonging to Plaintiffs  
24 and the Class.

25 130. Defendants knew or should have known they inadequately safeguarded  
26 this information.

27 131. Defendants knew that a breach of its systems would inflict millions of  
28 dollars of damages upon Plaintiffs and Class members, and Defendants were therefore  
charged with a duty to adequately protect this critically sensitive information.

1           132. Defendants had a special relationship with Plaintiffs and Class members.  
2 Plaintiffs' and Class members' highly sensitive PII and medical information was  
3 entrusted to Defendants on the understanding that adequate security precautions  
4 would be taken to protect the PII and medical information. Moreover, only  
5 Defendants had the ability to protect its systems and the PII stored on them from  
6 attack.

7           133. Defendants' own conduct also created a foreseeable risk of harm to  
8 Plaintiffs, Class members, and their PII. Defendants' misconduct included failing to:  
9 (1) secure their systems, servers and networks, despite knowing their vulnerabilities,  
10 (2) comply with industry standard security practices, (3) implement adequate system  
11 and event monitoring, and (4) implement the safeguards, policies, and procedures  
12 necessary to prevent this type of data breach.

13           134. Defendants breached their duties to Plaintiffs and Class members by  
14 failing to provide fair, reasonable, or adequate cyber networks and data security  
15 practices to safeguard the PII belonging to Plaintiffs and the Class.

16           135. Defendants breached their duties to Plaintiffs and the Class by creating  
17 a foreseeable risk of harm through the misconduct previously described.

18           136. Defendants breached the duties they owed to Plaintiffs and Class  
19 members by failing to implement proper technical systems or security practices that  
20 could have prevented the unauthorized access of PII.

21           137. The law further imposes an affirmative duty on Defendants to timely  
22 disclose the unauthorized access and theft of the PII belonging to Plaintiffs and the  
23 Class so that Plaintiffs and the Class can take appropriate measures to mitigate  
24 damages, protect against adverse consequences, and thwart future misuse of their PII.

25           138. Defendants breached the duties they owed to Plaintiffs and the Class by  
26 failing to disclose timely and accurately to Plaintiffs and Class members that their PII  
27 had been improperly acquired or accessed.

28           139. Defendants breached their duty to timely notify Plaintiffs and Class



1 members of the Data Breach by failing to provide direct notice to Plaintiffs and the  
2 Class concerning the Data Breach until on or about February 1, 2023.

3 140. As a direct and proximate result of Defendants' conduct, Plaintiffs and  
4 the Class have suffered a drastically increased risk of identity theft, relative to both  
5 the time period before the breach, as well as to the risk born by the general public, as  
6 well as other damages, including but not limited to time and expenses incurred in  
7 mitigating the effects of the Data Breach.

8 141. As a direct and proximate result of Defendants' negligent conduct,  
9 Plaintiffs and the Class have suffered injury and are entitled to damages in an amount  
10 to be proven at trial.

11 **COUNT II -- Negligence Per Se**  
12 **(By Plaintiffs on behalf of the Class, or, in the alternative, the California**  
13 **Subclass)**

14 142. Plaintiffs incorporate and realleges all allegations above as if fully set  
15 forth herein.

16 143. This count is brought on behalf of all Class members.

17 144. HIPAA obligates Covered Entities and Business Associates to "have in  
18 place appropriate administrative, technical, and physical safeguards to protect the  
19 privacy of protected health information" and "must reasonably safeguard protected  
20 health information." 45 CFR § 164.530(c).

21 145. In the event of a data breach, HIPAA obligates Covered Entities and  
22 Business Associates to notify affected individuals, prominent media outlets, and the  
23 Secretary of the Department of Health and Human Services of the data breach without  
24 unreasonable delay and in no event later than 60 days after discovery of the data  
25 breach. 45 CFR § 164.400, *et seq.*

26 146. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45,  
27 prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and  
28 enforced by the FTC, the unfair act or practice by companies, such as Defendants, of

1 failing to use reasonable measures to protect PII. Various FTC publications and orders  
2 also form the basis of Defendants' duty.

3 147. The California Customer Records Act ("CCRA"), Cal. Civ. Code  
4 § 1798.80, *et seq.*, requires that entities in possession of PII take reasonable measures  
5 to protect the PII, and timely and fully disclose any breach of the security of the PII  
6 in the entity's possession.

7 148. Furthermore, the California Unfair Competition Law ("UCL") Cal. Bus.  
8 & Prof. Code § 17200, *et seq.*, prohibits, inter alia, "any unlawful, unfair, or fraudulent  
9 business act or practice."

10 149. In addition to the FTC rules and regulations, the CCRA, and the UCL,  
11 other states and jurisdictions where victims of the Data Breach are located require that  
12 Defendants protect PII from unauthorized access and disclosure, and timely notify the  
13 victim of a data breach.

14 150. Defendants violated HIPAA, the CCRA, the UCL, and FTC rules and  
15 regulations obligating companies to use reasonable measures to protect PII by failing  
16 to comply with applicable industry standards, and by unduly delaying reasonable  
17 notice of the actual breach. Defendants' conduct was particularly unreasonable given  
18 the nature and amount of PII they obtained and stored, the foreseeable consequences  
19 of a Data Breach and the exposure of Plaintiffs' and Class members' sensitive PII.

20 151. Defendants' violations of HIPAA, the CCRA, the UCL, FTC rules and  
21 other applicable statutes, rules, and regulations constitutes negligence *per se*.

22 152. Plaintiffs and the Class are within the category of persons HIPAA, the  
23 CCRA, the UCL, and the FTC Act were intended to protect.

24 153. The harm that occurred as a result of the Data Breach described herein  
25 is the type of harm HIPAA, the CCRA, the UCL, and the FTC Act were intended to  
26 guard against.

27 154. As a direct and proximate result of Defendants' negligence *per se*,  
28 Plaintiffs and the Class have been damaged as described herein, continue to suffer

1 injuries as detailed above, are subject to the continued risk of exposure of their PII in  
 2 Defendants' possession, and are entitled to damages in an amount to be proven at trial.

3 **COUNT III — Breach of Implied Contract**  
 4 **(By Plaintiffs on behalf of the Class, or, in the alternative, the California**  
 5 **Subclass)**

6 155. Plaintiffs incorporate and reallege all allegations above as if fully set  
 7 forth herein.

8 156. This count is brought on behalf of all Class members.

9 157. Plaintiffs and the Class provided Defendants with their PII and medical  
 10 information.

11 158. By providing their PII and medical information, and upon Defendants'  
 12 acceptance of such information, Plaintiffs and the Class, on one hand, and Defendants,  
 13 on the other hand, entered into implied-in-fact contracts for the provision of data  
 14 security, separate and apart from any express contract entered into between the  
 15 parties.

16 159. The implied contracts between Defendants and Plaintiffs and Class  
 17 members obligated Defendants to take reasonable steps to secure, protect, safeguard,  
 18 and keep confidential Plaintiffs' and Class members' PII and medical information.  
 19 The terms of these implied contracts are described in federal laws, state laws, and  
 20 industry standards, as alleged above. Defendants expressly adopted and assented to  
 21 these terms in its public statements, representations and promises as described above.

22 160. The implied contracts for data security also obligated Defendants to  
 23 provide Plaintiffs and Class members with prompt, timely, and sufficient notice of  
 24 any and all unauthorized access or theft of their PII and medical information.

25 161. Defendants breached the implied contracts by failing to take, develop  
 26 and implement adequate policies and procedures to safeguard, protect, and secure the  
 27 PII and medical information belonging to Plaintiffs and Class members; allowing  
 28 unauthorized persons to access Plaintiffs' and Class members' PII; and failing to  
 provide prompt, timely, and sufficient notice of the Data Breach to Plaintiffs and Class

1 members, as alleged above.

2 162. As a direct and proximate result of Defendants' breaches of the implied  
3 contracts, Plaintiffs and the Class have been damaged as described herein, will  
4 continue to suffer injuries as detailed above due to the continued risk of exposure of  
5 their PII and medical information in Defendants possession, and are entitled to  
6 damages in an amount to be proven at trial.

7 **COUNT IV — Bailment**  
8 **(By Plaintiffs on behalf of the Class, or, in the alternative, the California**  
9 **Subclass)**

10 163. Plaintiffs incorporate and reallege all allegations above as if fully set  
11 forth herein.

12 164. This count is brought on behalf of all Class members.

13 165. Plaintiffs' and Class members' PII was provided to Defendants.

14 166. In delivering their PII and, Plaintiffs and Class members intended and  
15 understood that their PII would be adequately safeguarded and protected.

16 167. Defendants accepted Plaintiffs' and Class members' PII.

17 168. By accepting possession of Plaintiffs' and Class members' PII,  
18 Defendants understood that Plaintiffs and the Class expected their PII to be adequately  
19 safeguarded and protected. Accordingly, a bailment (or deposit) was established for  
20 the mutual benefit of the parties.

21 169. During the bailment (or deposit), Defendants owed a duty to Plaintiffs  
22 and the Class to exercise reasonable care, diligence, and prudence in protecting their  
23 PII.

24 170. Defendants breached their duty of care by failing to take appropriate  
25 measures to safeguard and protect Plaintiffs' and Class members' PII, resulting in the  
26 unlawful and unauthorized access to and misuse of Plaintiffs' and Class members'  
27 PII.

28 171. Defendants further breached their duty to safeguard Plaintiffs' and Class

1 members' PII by failing to timely notify them that their PII had been compromised as  
2 a result of the Data Breach.

3 172. Defendants failed to return, purge, or delete the PII belonging to  
4 Plaintiffs and Class members at the conclusion of the bailment (or deposit) and within  
5 the time limits allowed by law.

6 173. As a direct and proximate result of Defendants' breach of their duties,  
7 Plaintiffs and the Class suffered consequential damages that were reasonably  
8 foreseeable to Defendants, including but not limited to the damages set forth herein.

9 174. As a direct and proximate result of Defendants' breach of their duty,  
10 Plaintiffs' and Class members PII that was entrusted to Defendants during the  
11 bailment (or deposit) was damaged and its value diminished.

12 **COUNT V — Violation of the California Unfair Competition Law**  
13 **(By Plaintiffs on behalf of the Class, or, in the alternative, the California**  
14 **Subclass)**

15 175. Plaintiffs incorporate and reallege all allegations above as if fully set  
16 forth herein.

17 176. This count is brought on behalf of the California Subclass.

18 177. The California Unfair Competition Law ("UCL") Cal. Bus. & Prof. Code  
19 §17200, *et seq.*, prohibits, inter alia, "any unlawful, unfair, or fraudulent business act  
20 or practice." Cal. Bus. & Prof. Code §17200.

21 178. Defendants engaged in unlawful, unfair, and fraudulent business acts or  
22 practices in violation of the UCL.

23 179. Defendants' acts, omissions, and conduct were "unlawful" because they  
24 violated the FTC Act and were negligent.

25 180. Defendants' acts, omissions, and conduct were also "unlawful" because  
26 they violated the California Customer Records Act ("CCRA"), Cal. Civ. Code §  
27 1798.80, *et seq.* Defendants failed to take reasonable measures to protect Plaintiffs'  
28 and Class members' PII, in violation of Cal. Civ. Code § 1798.81.5. Defendants also

1 failed to timely and fully disclose the extent of the Data Breach in the Notice sent to  
2 Plaintiffs and Class members, in violation of Cal. Civ. Code § 1798.82.

3 181. Defendants' acts, omissions, and conduct were also "unlawful" because  
4 they violated the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §  
5 1798.150(a), and the California Confidentiality of Medical Information Act  
6 ("CMIA"), Cal. Civ. Code §56.10(a), by failing to implement proper procedures and  
7 failing to safeguard Plaintiffs' and Class members PII and confidential medical  
8 records.

9 182. Defendants' acts, omissions, and conduct were "unfair" because they  
10 offend public policy and constitute immoral, unethical, and unscrupulous activities  
11 that caused substantial injury, including to Plaintiffs and Class members. The gravity  
12 of harm resulting from Defendants' conduct outweighs any potential benefits  
13 attributable to the conduct and there were reasonably available alternatives to further  
14 Defendants' legitimate business interests. Defendants' unfair acts and practices  
15 include, but are not limited to:

- 16 a. Failing to implement and maintain reasonable security and privacy  
17 measures to protect Plaintiffs' and Class members' PII, which was a  
18 direct and proximate cause of the Data Breach;
- 19 b. Failing to identify foreseeable security and privacy risks, remediate  
20 identified security and privacy risks, and adequately improve security  
21 and privacy measures following previous cybersecurity incidents in  
22 the industry, which were direct and proximate causes of the Data  
23 Breach;
- 24 c. Failing to comply with common law and statutory duties pertaining to  
25 the security and privacy of Plaintiffs' and Class members' PII,  
26 including but not limited to duties imposed by HIPAA, the CCRA, the  
27 CCPA, the CMIA, and the FTC Act, which were direct and proximate  
28 causes of the Data Breach;

- d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that they would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and the Class members' PII;
- f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Class members' PII;
- g. Omitting, suppressing, and concealing the material fact that they did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' PII; and
- h. Failing to promptly and adequately notify Plaintiffs and Class members that their PII was accessed by unauthorized persons in the Data Breach.

183. Defendants engaged in fraudulent business practices by making material misrepresentations and by failing to disclose material information regarding Defendants' deficient security policies and practices, the security of the PII of Plaintiffs and Class members, and the Data Breach.

184. Defendants had exclusive knowledge of material information regarding their deficient security policies and practices, and regarding the security of the PII of Plaintiffs and Class members. This exclusive knowledge includes, but is not limited to, information that Defendants received through internal and other non-public audits and that the PII of Plaintiffs and Class members was vulnerable.

185. Defendants also had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

186. Defendants also had exclusive knowledge about the length of time that



1 it maintained former patients' PII.

2 187. Defendants failed to disclose the material information it had regarding  
3 their deficient security policies and practices, and regarding the security of the PII of  
4 Plaintiffs and Class members. For example, even though Defendants have long known  
5 that its security policies and practices were substandard and deficient, and that the PII  
6 of Plaintiffs and Class members was vulnerable as a result, Defendants failed to  
7 disclose this information to Plaintiffs and Class members. Likewise, during the days  
8 and weeks following the Data Breach, Defendants failed to disclose information that  
9 it had regarding the extent and nature of the Data Breach.

10 188. Defendants had a duty to disclose the material information that they had  
11 because, *inter alia*, they had exclusive knowledge of the information, they actively  
12 concealed the information, and because Defendants were in a fiduciary position by  
13 virtue of the fact that Defendants collected and maintained Plaintiffs' and Class  
14 members' financial information, medical information, and other PII.

15 189. Defendants' representations and omissions were material because they  
16 were likely to deceive reasonable individuals about the adequacy of Defendants' data  
17 security and its ability to protect the confidentiality of current and former employees'  
18 PII.

19 190. Had Defendants disclosed to Plaintiffs and Class members that its data  
20 systems were not secure and, thus, vulnerable to attack, Defendants would have been  
21 unable to continue in business as medical groups without adopting reasonable data  
22 security measures and complying with the law. Instead, Defendants received,  
23 maintained, and compiled Plaintiffs' and Class members' PII without advising them  
24 that Defendants' data security practices were insufficient to maintain the safety and  
25 confidentiality of their PII. Accordingly, Plaintiffs and the Class members acted  
26 reasonably in relying on Defendants' misrepresentations and omissions, the truth of  
27 which they could not have discovered.

28 191. Defendants' practices were also contrary to legislatively declared and

1 public policies that seek to protect data and ensure that entities who solicit or are  
2 entrusted with personal data utilize appropriate security measures, as reflected in laws  
3 like CCRA, CCPA, and FTC Act.

4 192. The injuries suffered by Plaintiffs and Class members greatly outweigh  
5 any potential countervailing benefit to consumers or to competition, and are not  
6 injuries that Plaintiffs and Class members should have reasonably avoided.

7 193. The damages, ascertainable losses and injuries, including to their money  
8 or property, suffered by Plaintiffs and Class members as a direct result of Defendants'  
9 unlawful, unfair, and fraudulent acts and practices as set forth in this Complaint  
10 include, without limitation:

- 11 a. unauthorized charges on their debit and credit card accounts;
- 12 b. theft of their PII;
- 13 c. costs associated with the detection and prevention of identity theft and  
14 unauthorized use of their financial accounts;
- 15 d. loss of use of and access to their account funds and costs associated  
16 with the inability to obtain money from their accounts or being limited  
17 in the amount of money they were permitted to obtain from their  
18 accounts, including missed payments on bills and loans, late charges  
19 and fees, and adverse effects on their credit including adverse effects  
20 on their credit scores and adverse credit notations;
- 21 e. costs associated with time spent and the loss of productivity from  
22 taking time to address and attempt to ameliorate and mitigate the  
23 actual and future consequences of the Data Breach, including without  
24 limitation finding fraudulent charges, cancelling and reissuing cards,  
25 purchasing credit monitoring and identity theft protection, imposition  
26 of withdrawal and purchase limits on compromised accounts, and the  
27 stress, nuisance and annoyance of dealing with all issues resulting  
28 from the Data Breach;

- 1 f. the imminent and certainly impending injury flowing from potential  
 2 fraud and identity theft posed by their PII being placed in the hands of  
 3 criminals;  
 4 g. damages to and diminution in value of their personal information  
 5 entrusted to Defendants, and with the understanding that Defendants  
 6 would safeguard their data against theft and not allow access and  
 7 misuse of their data by others; and  
 8 h. the continued risk to their PII, which remains in the possession of  
 9 Defendants and which is subject to further breaches so long as  
 10 Defendants fail to undertake appropriate and adequate measures to  
 11 protect data in their possession.

12 194. Plaintiffs and Class members seek all monetary and non-monetary relief  
 13 allowed by law, including actual or nominal damages; declaratory and injunctive  
 14 relief, including an injunction barring Defendants from disclosing their PII without  
 15 their consent; reasonable attorneys' fees and costs; and any other relief that is just and  
 16 proper.

17 **COUNT VI — Violation of California Customer Records Act**  
 18 **(By Plaintiffs and the California Subclass)**

19 195. Plaintiffs incorporate and reallege all allegations above as if fully set  
 20 forth herein.

21 196. This count is brought on behalf of all California Subclass members.

22 197. Cal. Civ. Code § 1798.81.5 of the California Customer Records Act  
 23 (“CCRA”) provides that “to ensure that personal information about California  
 24 residents is protected,” businesses maintaining the personal information of California  
 25 residents “shall implement and maintain reasonable security procedures and practices  
 26 appropriate to the nature of the information, to protect the personal information from  
 27 unauthorized access, destruction, use, modification, or disclosure.”

28 198. Defendants failed to take reasonable measures to protect Plaintiffs’ and

1 Class members' PII, in violation of Cal. Civ. Code § 1798.81.5.

2 199. Further, the CCRA requires that "[a] person or business that maintains  
3 computerized data that includes personal information that the person or business does  
4 not own shall notify the owner or licensee of the information of the breach of the  
5 security of the data immediately following discovery, if the personal information was,  
6 or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ.  
7 Code § 1798.82(b).

8 200. Defendants did not immediately notify Plaintiffs and the California  
9 Subclass of the Data Breach upon their discovery, and instead waited almost two  
10 months to provide notice.

11 201. Defendants also failed to timely and fully disclose the extent of the Data  
12 Breach in the Notice sent to Plaintiffs and Class members, in violation of Cal. Civ.  
13 Code § 1798.82.

14 202. Defendants' violations of Cal. Civ. Code §§ 1798.81.5 and 1798.82 are  
15 a direct and proximate result of the Data Breach.

16 203. Plaintiffs and California Subclass members seek all monetary and non-  
17 monetary relief allowed by law, including actual or nominal damages; declaratory and  
18 injunctive relief, including an injunction barring Defendants from disclosing their PII  
19 without their consent; reasonable attorneys' fees and costs; and any other relief that  
20 is just and proper.

21 **COUNT VII -- Violation of the California Consumer Privacy Act**  
22 **(By Plaintiffs and the California Subclass)**

23 204. Plaintiffs incorporate and reallege all allegations above as if fully set  
24 forth herein.

25 205. This count is brought on behalf of all California Subclass members.

26 206. Cal. Civ. Code § 1798.150(a) of the California Consumer Privacy Act  
27 ("CCPA") provides that "[a]ny consumer whose nonencrypted and nonredacted  
28 personal information, as defined in subparagraph (A) of paragraph (1) of subdivision

1 (d) of Section 1798.81.5 . . . is subject to an unauthorized access and exfiltration, theft,  
2 or disclosure as a result of the business’s violation of the duty to implement and  
3 maintain reasonable security procedures and practices appropriate to the nature of the  
4 information to protect the personal information may institute a civil action” for  
5 statutory damages, actual damages, injunctive relief, declaratory relief and any other  
6 relief the court deems proper.

7 207. Plaintiffs are “consumers” as defined by Cal. Civ. Code § 1798.140(g)  
8 because they are natural persons who reside in California.

9 208. Defendants are “business[es]” as defined by Cal. Civ. Code §  
10 1798.140(c) because Defendants are corporations organized for the profit or financial  
11 benefit of their shareholders or owners and have gross annual revenues in excess of  
12 twenty-five million dollars.

13 209. Defendants failed to take sufficient and reasonable measures to  
14 safeguard their data security systems and protect Plaintiffs’ and Class members’  
15 highly sensitive personal information and medical data from unauthorized access.  
16 Defendants’ failure to maintain adequate data protections subjected Plaintiffs’ and the  
17 Class’ nonencrypted and nonredacted sensitive personal information to exfiltration  
18 and disclosure by malevolent actors.

19 210. Defendants’ violations of Cal. Civ. Code § 1798.150(a) are a direct and  
20 proximate result of the Data Breach.

21 211. Plaintiffs and California Subclass members seek all monetary and non-  
22 monetary relief allowed by law, including actual or nominal damages; declaratory and  
23 injunctive relief, including an injunction barring Defendants from disclosing their PII  
24 without their consent; reasonable attorneys’ fees and costs; and any other relief that  
25 is just and proper.

**COUNT VIII — Violation of California Confidentiality  
of Medical Information Act**

**(By Plaintiffs and the California Subclass)**

212. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

213. This count is brought on behalf of all California Subclass members.

214. Cal. Civ. Code §56.10(a) of the California Confidentiality of Medical Information Act (“CMIA”) provides that “[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]”

215. The CMIA further requires that “[e]very provider of health care, health care service plan, pharmaceutical company, or contractor who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care, health care service plan, pharmaceutical company, or contractor who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.” Cal. Civ. Code §56.101(a).

216. Defendants are a “provider of health care” because they are “organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care.” Cal. Civ. Code §56.06(a).

217. Plaintiffs are “patient[s]” because they are “natural person[s], whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.” Cal. Civ. Code §56.05(1).

218. Defendants failed to safeguard the protected medical information of Plaintiffs and the Class by maintaining inadequate data security networks, allowing

1 unauthorized parties to access the protected medical information of Plaintiffs and the  
2 Class, and failing to preserve the confidentiality of the protected medical information  
3 of Plaintiffs and the Class.

4 219. Defendants allowed third parties to access, exfiltrate, and disclose  
5 Plaintiffs' and Class members' protected health and personal information without  
6 their consent or knowledge. Defendants negligently represented that such information  
7 would be protected from such unauthorized access.

8 220. Defendants' violations of Cal. Civ. Code §§ 56.10(a) and 56.101(a) are  
9 a direct and proximate result of the Data Breach.

10 221. Plaintiffs and California Subclass members seek all monetary and non-  
11 monetary relief allowed by law, including actual or nominal damages; declaratory and  
12 injunctive relief, including an injunction barring Defendants from disclosing their PII  
13 without their consent; reasonable attorneys' fees and costs; and any other relief that  
14 is just and proper.

15 **COUNT IX — Violation of State Data Breach Statutes**

16 **(By Plaintiffs on behalf of the Class)**

17 222. Plaintiffs incorporate and reallege all allegations above as if fully set  
18 forth herein.

19 223. This count is brought on behalf of all Class members.

20 224. Defendants are a corporation that owns, maintains, and records PII, and  
21 computerized data including PII, about its current and former patients, including  
22 Plaintiffs and Class members.

23 225. Defendants are in possession of PII belonging to Plaintiffs and Class  
24 members and are responsible for reasonably safeguarding that PII consistent with the  
25 requirements of the applicable laws pertaining hereto.

26 226. Defendants failed to safeguard, maintain, and dispose of, as required, the  
27 PII within its possession, custody, or control as discussed herein, which it was  
28 required to do by all applicable State laws.



227. Defendants, knowing and/or reasonably believing that Plaintiffs' and Class members' PII was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiffs and Class members as required by the following data breach statutes.

228. Defendants' failure to provide timely and accurate notice of the Data Breach violated the following state data breach statutes:

- a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;
- b. Ark. Code Ann. § 4-110-105(a), *et seq.*;
- c. Cal. Civ. Code § 1798.80, *et seq.*;
- d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;
- e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;
- f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;
- g. D.C. Code § 28-3852(a), *et seq.*;
- h. Fla. Stat. Ann. § 501.171(4), *et seq.*;
- i. Ga. Code Ann. § 10-1-912(a), *et seq.*;
- j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;
- k. Idaho Code Ann. § 28-51-105(1), *et seq.*;
- l. Illinois Statute 815 ILCS 530/1, *et seq.*;
- m. Iowa Code Ann. § 715C.2(1), *et seq.*;
- n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;
- o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;
- p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;
- q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;
- r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;
- s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;
- t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;
- u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;
- v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

1 w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;  
 2 x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;  
 3 y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;  
 4 z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;  
 5 aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;  
 6 bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;  
 7 cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;  
 8 dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), *et seq.*;  
 9 ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;  
 10 ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;  
 11 gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;  
 12 hh. Utah Code Ann. § 13-44-202(1), *et seq.*;  
 13 ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;  
 14 jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;  
 15 kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and  
 16 ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

17 229. As a result of Defendants' failure to reasonably safeguard Plaintiffs' and  
 18 Class members' PII, and the failure to provide reasonable and timely notice of the  
 19 Data Breach to Plaintiffs and Class members, Plaintiffs and the Class have been  
 20 damaged as described herein, continue to suffer injuries as detailed above, are subject  
 21 to the continued risk of exposure of their PII in Defendants' possession, and are  
 22 entitled to damages in an amount to be proven at trial.

23 **COUNT X – Violation of State Consumer Protection Statutes**  
 24 **(On behalf of Plaintiffs and the Class)**

25 230. Plaintiffs incorporate and reallege all allegations above as if fully set  
 26 forth herein.

27 231. This count is brought on behalf of all Class members.

28 232. Defendants are a "person" as defined in the relevant state consumer

1 statutes.

2 233. Defendants engaged in the conduct alleged herein that was intended to  
3 result, and which did result, in the trade and commerce with Plaintiffs and Class  
4 members. Defendants are engaged in, and their acts and omissions affect, trade and  
5 commerce. Further, Defendants' conduct implicates consumer protection concerns  
6 generally.

7 234. Defendants' acts, practices and omissions were done in the course of  
8 Defendants' business of marketing, facilitating, offering for sale, and selling goods  
9 and services throughout the United States.

10 235. Defendants' unlawful, unfair, deceptive, fraudulent and/or  
11 unconscionable acts and practices include:

- 12 a. Failing to implement and maintain reasonable security and privacy  
13 measures to protect Plaintiffs' and Class members' PII, which was a  
14 direct and proximate cause of the Data Breach;
- 15 b. Failing to identify foreseeable security and privacy risks, remediate  
16 identified security and privacy risks, and adequately improve security  
17 and privacy measures following previous cybersecurity incidents in  
18 the industry, which was a direct and proximate cause of the Data  
19 Breach;
- 20 c. Failing to comply with common law and statutory duties pertaining to  
21 the security and privacy of Plaintiffs' and Class members' PII,  
22 including but not limited to duties imposed by the FTC Act and similar  
23 state laws, rules, and regulations, which was a direct and proximate  
24 cause of the Data Breach;
- 25 d. Misrepresenting that they would protect the privacy and  
26 confidentiality of Plaintiffs' and Class members' PII, including by  
27 implementing and maintaining reasonable security measures;
- 28 e. Misrepresenting that they would comply with common law, statutory,

1 and self-imposed duties pertaining to the security and privacy of  
2 Plaintiffs' and the Class members' PII;

3 f. Omitting, suppressing, and concealing the material fact that they did  
4 not reasonably or adequately secure Plaintiffs' and Class members'  
5 PII;

6 g. Omitting, suppressing, and concealing the material fact that they did  
7 not comply with common law, statutory, and self-imposed duties  
8 pertaining to the security and privacy of Plaintiffs' and Class  
9 members' PII; and

10 h. Failing to promptly and adequately notify Plaintiffs and Class  
11 members that their PII was accessed by unauthorized persons in the  
12 Data Breach.

13 236. By engaging in such conduct and omissions of material facts, Defendants  
14 have violated state consumer laws prohibiting representing that "goods or services  
15 have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities  
16 that they do not have," representing that "goods and services are of a particular  
17 standard, quality or grade, if they are of another", and/or "engaging in any other  
18 conduct which similarly creates a likelihood of confusion or of misunderstanding";  
19 and state consumer laws prohibiting unfair methods of competition and unfair,  
20 deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

21 237. Defendants' representations and omissions were material because they  
22 were likely to deceive reasonable persons about the adequacy of Defendants' data  
23 security and ability to protect the confidentiality of PII.

24 238. Defendants intentionally, knowingly, and maliciously misled Plaintiffs  
25 and Class members and induced them to rely on their misrepresentations and  
26 omissions.

27 239. Had Defendants disclosed that their data systems were not secure and,  
28 thus, vulnerable to attack, they would have been unable to continue in business and

1 they would have been forced to adopt reasonable data security measures and comply  
2 with the law. Instead, Defendants received, maintained, and compiled Plaintiffs' and  
3 Class members' PII without advising that Defendants' data security practices were  
4 insufficient to maintain the safety and confidentiality of their PII. Accordingly,  
5 Plaintiffs and the Class members acted reasonably in relying on Defendants'  
6 misrepresentations and omissions, the truth of which they could not have discovered.

7 240. Past breaches within the industry put Defendants on notice that their  
8 security and privacy protections were inadequate.

9 241. Defendants' practices were also contrary to legislatively declared and  
10 public policies that seek to protect consumer data and ensure that entities who solicit  
11 or are entrusted with personal data utilize appropriate security measures, as reflected  
12 in laws like the CCRA, the UCL, and the FTC Act.

13 242. The harm these practices caused to Plaintiffs and Class members  
14 outweighed their utility, if any.

15 243. The damages, ascertainable losses and injuries, including to their money  
16 or property, suffered by Plaintiffs and Class members as a direct result of Defendants'  
17 unfair methods of competition and unfair, deceptive, fraudulent, unconscionable  
18 and/or unlawful acts or practices as set forth herein include, without limitation:

- 19 a. unauthorized charges on their debit and credit card accounts;
- 20 b. theft of their PII;
- 21 c. costs associated with the detection and prevention of identity theft and
- 22 unauthorized use of their financial accounts;
- 23 d. loss of use of and access to their account funds and costs associated
- 24 with the inability to obtain money from their accounts or being limited
- 25 in the amount of money they were permitted to obtain from their
- 26 accounts, including missed payments on bills and loans, late charges
- 27 and fees, and adverse effects on their credit including adverse effects
- 28 on their credit scores and adverse credit notations;

- 1 e. costs associated with time spent and the loss of productivity from  
2 taking time to address and attempt to ameliorate and mitigate the  
3 actual and future consequences of the Data Breach, including without  
4 limitation finding fraudulent charges, cancelling and reissuing cards,  
5 purchasing credit monitoring and identity theft protection, imposition  
6 of withdrawal and purchase limits on compromised accounts, and the  
7 stress, nuisance and annoyance of dealing with all issues resulting  
8 from the Data Breach;
- 9 f. the imminent and certainly impending injury flowing from potential  
10 fraud and identity theft posed by their PII being placed in the hands of  
11 criminals;
- 12 g. damages to and diminution in value of their personal and medical  
13 information entrusted to Defendants and with the understanding that  
14 Defendants would safeguard their data against theft and not allow  
15 access and misuse of their data by others; and
- 16 h. the continued risk to their PII, which remains in the possession of  
17 Defendants and which is subject to further breaches so long as  
18 Defendants fail to undertake appropriate and adequate measures to  
19 protect data in its possession.

20 244. Defendants' conduct described herein, including without limitation,  
21 Defendants' failure to maintain adequate computer systems and data security  
22 practices to safeguard Plaintiffs' and Class members' PII, Defendants' failure to  
23 disclose the material fact that they did not have adequate computer systems and  
24 safeguards to adequately protect Plaintiffs' and Class members' PII, Defendants'  
25 failure to provide timely and accurate notice to of the material fact of the Data Breach,  
26 and Defendants' continued acceptance of Plaintiffs' and Class members' PII  
27 constitutes unfair methods of competition and unfair, deceptive, unconscionable,  
28 fraudulent and/or unlawful acts or practices in violation of the following state

1 consumer statutes:

- 2 a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5),  
3 (7) and (27), *et seq.*;
- 4 b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;
- 5 c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-  
6 88-107(a)(1)(10) and 4-88-108(1)(2), *et seq.*;
- 7 d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750,  
8 *et seq.*, and the California Unfair Competition Law, Cal. Bus. and Prof.  
9 Code, § 17200, *et seq.*;
- 10 e. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-  
11 110(b), *et seq.*;
- 12 f. The Delaware Deceptive Trade Practices Act, Del. Code Ann. Title 6,  
13 § 2532(5) and (7), *et seq.*, and the Delaware Consumer Fraud Act, Del.  
14 Code Ann. Title 6 § 2513, *et seq.*;
- 15 g. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann.  
16 § 501.204(1), *et seq.*;
- 17 h. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-  
18 393(a) and (b)(2), (5) and (7), *et seq.*;
- 19 i. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§  
20 481A-3(a)(5), (7) and (12), *et seq.*; and the Hawaii Consumer  
21 Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq.*;
- 22 j. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7),  
23 (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;
- 24 k. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815  
25 Ill. Stat. § 505/2, *et seq.*;
- 26 l. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-  
27 3(a) and (b)(1) and (2), *et seq.*;
- 28 m. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, *et seq.*;



- n. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), *et seq.*;
- o. The Kentucky Consumer Protection Act, K.R.S. § 367.170(1) and (2), *et seq.*;
- p. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq.*;
- q. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), *et seq.*, and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, *et seq.*;
- r. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq.*;
- s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq.*;
- t. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e),(s) and (cc), *et seq.*;
- u. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), *et seq.*, the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);
- v. The Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-5(1), (2)(e) and (g), *et seq.*;
- w. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq.*;
- x. The Montana Unfair Trade Practices and Consumer Protection Act, MCA §§ 30-14-103, *et seq.*;
- y. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq.*;

- 1 z. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann.
- 2 § 598.0915(5) and (7), *et seq.*;
- 3 aa. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann.
- 4 § 358-A:2(v) and (vii), *et seq.*;
- 5 bb. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;
- 6 cc. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-
- 7 2(D)(5)(7) and (14) and 57-12-3, *et seq.*;
- 8 dd. New York Business Law, N.Y. Gen. Bus. Law § 349(a);
- 9 ee. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-
- 10 1.1(a), *et seq.*;
- 11 ff. The North Dakota Unlawful Sales or Advertising Practices Act, N.D.
- 12 Cent. Code § 51-15-02, *et seq.*;
- 13 gg. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann.
- 14 § 1345.02(A) and (B)(1) and (2), *et seq.*;
- 15 hh. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 753(5),
- 16 (7) and (20), *et seq.*; and the Oklahoma Deceptive Trade Practices Act,
- 17 78 Okl. Stat. Ann. § 53(A)(5) and (7), *et seq.*;
- 18 ii. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. §
- 19 646.608(1)(e)(g) and (u), *et seq.*;
- 20 jj. The Pennsylvania Unfair Trade Practices and Consumer Protection
- 21 Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq.*;
- 22 kk. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-
- 23 13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq.*;
- 24 ll. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-
- 25 5-20(a), *et seq.*;
- 26 mm. The South Dakota Deceptive Trade Practices Act and Consumer
- 27 Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq.*;
- 28 nn. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-

- 1                   104(a) and (b)(5) and (7);
- 2                   oo. The Texas Deceptive Trade Practices- Consumer Protection Act,
- 3                   V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq.*;
- 4                   pp. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-
- 5                   4(1) and (2)(a) and (b);
- 6                   qq. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq.*;
- 7                   rr. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-
- 8                   200(A)(5)(6) and (14), *et seq.*;
- 9                   ss. The Washington Consumer Protection Act, Wash. Rev. Code §
- 10                  19.86.020, *et seq.*;
- 11                  tt. The West Virginia Consumer Credit and Protection Act, W.V.A. Code
- 12                  § 46A-6-104, *et seq.*;
- 13                  uu. The Wisconsin Deceptive Trade Practices Act, W.S.A. § 100.20(1), *et*
- 14                  *seq.*; and
- 15                  vv. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-
- 16                  105(a), (i), (iii) and (xv), *et seq.*

17           245. Plaintiffs and Class members seek all monetary and non-monetary relief

18 allowed by law, including actual or nominal damages; declaratory and injunctive

19 relief, including an injunction barring Defendants from disclosing their PII without

20 their consent; reasonable attorneys' fees and costs; and any other relief that is just and

21 proper.

22                                   **COUNT XI — Intrusion Upon Seclusion**

23           **(By Plaintiffs on behalf of the Class, or, in the alternative, the California**

24                                   **Subclass)**

25           246. Plaintiffs incorporate and reallege all allegations above as if fully set

26 forth herein.

27           247. This count is brought on behalf of all Class members.

28           248. Plaintiffs bring this claim on behalf of persons who reside in Alabama,

1 Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida,  
2 Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine,  
3 Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico,  
4 North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah,  
5 Vermont, Washington, and West Virginia; and any other state that recognizes a claim  
6 for intrusion upon seclusion under the facts and circumstances alleged above (the  
7 “Intrusion Upon Seclusion States”).

8 249. Plaintiffs and Class members had a reasonable expectation of privacy in  
9 the PII that Defendants possessed and/or continues to possess.

10 250. By failing to keep Plaintiffs’ and Class members’ PII safe, and by  
11 misusing and/or disclosing their PII to unauthorized parties for unauthorized use,  
12 Defendants invaded Plaintiffs’ and Class members’ privacy by:

13 a. Intruding into their private affairs in a manner that would be highly  
14 offensive to a reasonable person; and

15 b. Publicizing private facts about Plaintiffs and Class members, which is  
16 highly offensive to a reasonable person.

17 251. Defendants knew, or acted with reckless disregard of the fact that, a  
18 reasonable person in Plaintiffs’ position would consider Defendants’ actions highly  
19 offensive.

20 252. Defendants invaded Plaintiffs’ and Class members’ right to privacy and  
21 intruded into Plaintiffs’ and Class members’ private affairs by misusing and/or  
22 disclosing their private information without their informed, voluntary, affirmative,  
23 and clear consent.

24 253. As a proximate result of such misuse and disclosures, Plaintiffs’ and  
25 Class members’ reasonable expectation of privacy in their PII was unduly frustrated  
26 and thwarted. Defendants’ conduct amounted to a serious invasion of Plaintiffs’ and  
27 Class members’ protected privacy interests.

28 254. In failing to protect Plaintiffs’ and Class members’ PII, and in misusing

1 and/or disclosing their PII, Defendants have acted with malice and oppression and in  
 2 conscious disregard of Plaintiffs' and the Class members rights to have such  
 3 information kept confidential and private, in failing to provide adequate notice, and  
 4 in placing its own economic, corporate, and legal interests above the privacy interests  
 5 of its millions of patients. Plaintiffs, therefore, seeks an award of damages, including  
 6 punitive damages, on behalf of Plaintiffs and the Class.

7  
**COUNT XII -- Unjust Enrichment**

8 **(By Plaintiffs on behalf of the Class, or, in the alternative, the California**  
 9 **Subclass)**

10 255. Plaintiffs incorporate and reallege all allegations above as if fully set  
 11 forth herein.

12 256. This count is brought on behalf of all Class members.

13 257. Plaintiffs and the Class have an interest, both equitable and legal, in their  
 14 PII and medical information that was collected and maintained by Defendants.

15 258. Defendants were benefitted by the conferral upon it of Plaintiffs' and  
 16 Class members' PII and by their ability to retain and use that information. Defendants  
 17 understood that it was in fact so benefitted.

18 259. Defendants also understood and appreciated that Plaintiffs' and Class  
 19 members' PII and medical information was private and confidential and its value  
 20 depended upon Defendants maintaining the privacy and confidentiality of that  
 21 information.

22 260. But for Defendants' willingness and commitment to maintain its privacy  
 23 and confidentiality, Plaintiffs and Class members would not have provide or  
 24 authorized their PII to be provided to Defendants, and Defendants would have been  
 25 deprived of the competitive and economic advantages it enjoyed by falsely claiming  
 26 that their data-security safeguards met reasonable standards. These competitive and  
 27 economic advantages include, without limitation, wrongfully gaining patients,  
 28 gaining the reputational advantages conferred upon it by Plaintiffs and Class

1 members, collecting excessive advertising and sales revenues as described herein,  
2 monetary savings resulting from failure to reasonably upgrade and maintain data  
3 technology infrastructures, staffing, and expertise raising investment capital as  
4 described herein, and realizing excessive profits.

5       261. As a result of Defendants' wrongful conduct as alleged herein (including,  
6 among other things, their deception of Plaintiffs, the Class, and the public relating to  
7 the nature and scope of the data breach; their failure to employ adequate data security  
8 measures; their continued maintenance and use of the PII belonging to Plaintiffs and  
9 Class members without having adequate data security measures; and its other conduct  
10 facilitating the theft of that PII) Defendants have been unjustly enriched at the expense  
11 of, and to the detriment of, Plaintiffs and the Class.

12       262. Defendants' unjust enrichment is traceable to, and resulted directly and  
13 proximately from, the conduct alleged herein, including the compiling and use of  
14 Plaintiffs' and Class members' sensitive PII, while at the same time failing to maintain  
15 that information secure from intrusion.

16       263. Under the common law doctrine of unjust enrichment, it is inequitable  
17 for Defendants to be permitted to retain the benefits they received, and are still  
18 receiving, without justification, from Plaintiffs and the Class in an unfair and  
19 unconscionable manner. Defendants' retention of such benefits under circumstances  
20 making it inequitable to do so constitutes unjust enrichment.

21       264. The benefit conferred upon, received, and enjoyed by Defendants was  
22 not conferred officiously or gratuitously, and it would be inequitable and unjust for  
23 Defendants to retain the benefit.

24       265. Defendants are therefore liable to Plaintiffs and the Class for restitution  
25 in the amount of the benefit conferred on Defendants as a result of their wrongful  
26 conduct, including specifically the value to Defendants of the PII and medical  
27 information that was accessed and exfiltrated in the Data Breach and the profits  
28 Defendants receive from the use and sale of that information.

**COUNT XIII -- Declaratory Judgment**

**(By Plaintiffs on behalf of the Class, or, in the alternative, the California Subclass)**

266. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

267. This count is brought on behalf of all Class members.

268. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

269. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' PII, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their PII. Plaintiffs allege that Defendants' data security measures remain inadequate.

270. Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

271. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendants continue to owe a legal duty to secure Plaintiffs' and Class members' PII, to timely notify them of any data breach, and to establish and implement data security measures that are adequate to secure PII.

272. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect Plaintiffs' and Class members' PII.

273. If an injunction is not issued, Plaintiffs and the Class will suffer



1 irreparable injury and lack an adequate legal remedy. The threat of another breach of  
 2 the PII in Defendants' possession, custody, and control is real, immediate, and  
 3 substantial. If another breach of Defendants' network, systems, servers, or  
 4 workstations occurs, Plaintiffs and the Class will not have an adequate remedy at law,  
 5 because many of the resulting injuries are not readily quantified and they will be  
 6 forced to bring multiple lawsuits to rectify the same conduct.

7 274. The hardship to Plaintiffs and the Class if an injunction does not issue  
 8 exceeds the hardship to Defendants if an injunction is issued. Among other things, if  
 9 another massive data breach occurs at Defendants, Plaintiffs and the Class will likely  
 10 be subjected to substantial identify theft and other damage. On the other hand, the  
 11 cost to Defendants of complying with an injunction by employing reasonable  
 12 prospective data security measures is relatively minimal, and Defendants have a pre-  
 13 existing legal obligation to employ such measures.

14 275. Issuance of the requested injunction will serve the public interest by  
 15 preventing another data breach at Defendants, thus eliminating additional injuries to  
 16 Plaintiffs and the thousands of Class members whose confidential information would  
 17 be further compromised.

#### 18 **PRAYER FOR RELIEF**

19 WHEREFORE, Plaintiffs, individually, and on behalf of all members of the  
 20 Class, respectfully requests that the Court enter judgment in their favor and against  
 21 Defendants, as follows:

- 22 A. That the Court certify this action as a class action, proper and
- 23 maintainable pursuant to Rule 23 of the Federal Rules of Civil
- 24 Procedure; declare that Plaintiffs are proper class representatives; and
- 25 appoint Plaintiffs' Counsel as Class Counsel;
- 26 B. That Plaintiffs be granted the declaratory relief sought herein;
- 27 C. That the Court grant permanent injunctive relief to prohibit Defendants
- 28 from continuing to engage in the unlawful acts, omissions, and practices

described herein;

D. That the Court award Plaintiffs and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiffs and the Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

**DEMAND FOR JURY TRIAL**

Plaintiffs, on behalf of themselves and the putative Class, demand a trial by jury on all issues so triable.

Date: February 28, 2023

Respectfully Submitted,

By: /s/ Jonathan M. Rotter

Jonathan M. Rotter (SBN 234137)

Pavithra Rajesh (SBN 323055)

**GLANCY PRONGAY & MURRAY LLP**

1925 Century Park East, Suite 2100

Los Angeles, California 90067

Telephone: (310) 201-9150

Facsimile: (310) 201-9160

jrotter@glancylaw.com

prajesh@glancylaw.com

1 Daniel O. Herrera (*pro hac vice* anticipated)  
2 Nickolas J. Hagman (*pro hac vice* anticipated)  
3 **CAFFERTY CLOBES MERIWETHER**  
4 **& SPRENGEL LLP**  
5 135 S. LaSalle, Suite 3210  
6 Chicago, Illinois 60603  
7 Telephone: (312) 782-4880  
8 Facsimile: (312) 782-4485  
9 dherrera@caffertyclobes.com  
10 nhagman@caffertyclobes.com

11 Bryan L. Clobes (*pro hac vice* anticipated)  
12 **CAFFERTY CLOBES MERIWETHER**  
13 **& SPRENGEL LLP**  
14 205 N. Monroe St.  
15 Media, PA 19063  
16 Telephone: (215) 864-2800  
17 Facsimile: (312) 782-4485  
18 bclobes@caffertyclobes.com

19 *Attorneys for Plaintiffs and the Proposed*  
20 *Class*